S. HRG. 113–295

THE CYBERSECURITY PARTNERSHIP BETWEEN THE PRIVATE SECTOR AND OUR GOVERNMENT: PROTECTING OUR NATIONAL AND ECONOMIC SECURITY

JOINT HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

AND THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

MARCH 7, 2013

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

88–180 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
MARK PRYOR, Arkansas
CLAIRE MCCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
MARK WARNER, Virginia
MARK BEGICH, Alaska
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
WILLIAM COWAN, Massachusetts

JOHN THUNE, South Dakota, *Ranking*
ROGER F. WICKER, Mississippi
ROY BLUNT, Missouri
MARCO RUBIO, Florida
KELLY AYOTTE, New Hampshire
DEAN HELLER, Nevada
DAN COATS, Indiana
TIM SCOTT, South Carolina
TED CRUZ, Texas
DEB FISCHER, Nebraska
RON JOHNSON, Wisconsin

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
JOHN WILLIAMS, *General Counsel*
DAVID SCHWIETERT, *Republican Staff Director*
NICK ROSSI, *Republican Deputy Staff Director*
REBECCA SEIDEL, *Republican General Counsel and Chief Investigator*

SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware, *Chairman*

CARL LEVIN, Michigan
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
MARK BEGICH, Alaska
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota

TOM COBURN, Oklahoma, *Ranking*
JOHN MCCAIN, Arizona
RON JOHNSON, Wisconsin
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire

RICHARD J. KESSLER, *Staff Director*
JOHN P. KILVINGTON, *Deputy Staff Director*
BETH M. GROSSMAN, *Chief Counsel*
KEITH B. ASHDOWN, *Republican Staff Director*
CHRISTOPHER J. BARKLEY, *Republican Deputy Staff Director*
ANDREW C. DOCKHAM, *Chief Counsel*

CONTENTS

WITNESSES

APPENDIX

THE CYBERSECURITY PARTNERSHIP BETWEEN THE PRIVATE SECTOR AND OUR GOVERNMENT: PROTECTING OUR NATIONAL AND ECONOMIC SECURITY

THURSDAY, MARCH 7, 2013

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committees met, pursuant to notice, at 2:30 p.m., in room SD–G50, Dirksen Senate Office Building, Hon. John D. Rockefeller IV, Chairman of the Commerce Committee, presiding.

OPENING STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

Chairman ROCKEFELLER. Ladies and gentlemen, this hearing will come to order.

I have one quick announcement to make—and that is, I was just told that we may have a vote on John Brennan, for the CIA, coming up within a relatively short period of time, so we need to be as efficient as possible. But, on the other hand, we can come back from that.

So, let me make my opening statement. And I know that Tom is coming.

Long ago, we made the decision in this country that private companies would build, and that they would own, our key transportation, communications, and energy networks. That was, and still is, a good decision. Given the opportunity to earn a reasonable profit on their investment, private companies build our railroads, our wireline telephone network, our aviation system, our pipelines, and so many other physical assets that we have. They were built by private corporations, private money, and are owned by them.

But, this isn't just our past, it's our future, too. With the encouragement and support of Federal, State, and local governments, private companies are hard at work today building the broadband network that will be the key to our country's success in the 21st century. What we have always asked these companies for in return is that they serve, not just the interests of their shareholders, but also the broader general interests of the country, however one wants to define that.

As those of us who serve on the Commerce Committee know well, getting big things done in this country, and in this body, is slow.

It's very slow. And it always takes, on really big stuff, the private sector and the public sector, working together. It just has to be that way. That's the kind of partnership we will need to address the grave new threat that our country faces today, which are cyber attacks, which, 4 years ago, were treated lightly, and today are still treated too lightly, in my judgment, but is the number one national security threat that the country faces.

Back in 2009, when I started working on this issue with Senator Olympia Snowe, cybersecurity was just an exotic idea. To some, it still is just that, or it's an idea to push aside and take up later. But, it is not. Almost every day, we read about another company, another Government agency that's been electronically attacked by adversaries trying to cause economic damage or searching for sensitive information, and getting it. It's not a threat that we can address through a traditional military response, of course, and it's not a threat that individual companies can handle through their normal risk mitigation practices. It's a threat that challenges our traditional notion of the public and private spheres. That's what makes it interesting.

A cyber attack against a government agency or a defense contractor is an attack against our nation. An attack against a private company dealing with—say, a water company—is an attack against our nation. So is it with an attack on a private company that provides power or clean water to millions of Americans; an attack against any of these pieces, even though they might be privately operated, is an attack against our nation's critical infrastructure and, therefore, against us, as a nation.

Since I've been working on this issue, I've had a lot of good and productive sessions with the private sector. But, you know what? We also have wasted an awful lot of time by turning an urgent national security issue into a partisan political fight. How one does that on the number one national security threat, I don't know, but somehow we've managed to do it.

Back in 2010, we passed, in the Commerce Committee, a cyber bill. We did it unanimously. And we did that because we didn't have any vote, everybody just agreed, and it zipped right through. However, we couldn't get enough votes, in 2012, to start debate, even, on this issue on the Senate floor even though the whole military and intelligence establishment was going crazy at our lack of movement.

The Obama administration got tired of waiting for us. I can't blame them. This is a problem that's growing worse every day. So, on February 12 of this year, the President released an Executive order that takes some very important steps—not enough, because he can't create the law that's necessary for some things, but they worked very hard to make this Executive order a welcoming invitation to the private sector to work together on this problem. It seeks to formalize and to strengthen the working relationships many companies already have with our cybersecurity experts in the Federal Government.

The Executive order starts a process with NIST—can NIST be helpful? I think this can be helpful. Some others don't think so, because it's called a "government agency." We're going to hear more about the Executive orders from our witnesses. The Senators sit-

ting in this dais today understand what an urgent issue this is. We all want to do something. We want to come together. We want to be ruled by our common sense, not by other interests. So, we have our work cut out.

[The prepared statement of Chairman Rockefeller follows:]

PREPARED STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA AND CHAIRMAN, U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

Long ago we made the decision that in this country, private companies would build and own our key transportation, communications, and energy networks. That was and still is a good decision. Given the opportunity to earn a reasonable profit on their investment, private companies built our railroads, our wireline telephone network, our aviation system, our pipelines, and many other physical assets that have fueled our country's phenomenal economic success. This isn't just our past. It's our future too. With the encouragement and support of federal, state, and local governments, private companies are hard at work today building the broadband network that will be key to our country's success in the 21st century.

What we have always asked these companies for in return is that they serve not just the narrow interests of their shareholders, but also the broader, general interests of this country. As those of us who serve on the Commerce Committee know very well, getting big things done in this country always requires a partnership between the public and private sectors. That's the kind of partnership we will need to address the grave new threat our country faces today—the threat of cyber attacks.

Back in 2009, when I started working on this issue with Senator Snowe, cybersecurity was an exotic idea. Today, four years later, it is a household word. Almost every day, we read about another company, or another government agency, that has been electronically attacked by adversaries trying to cause economic damage or searching for sensitive information.

It's not a threat we can address through a traditional military response, and it's not a threat that individual companies can handle through their normal risk mitigation practices. It's a threat that challenges our traditional notion of the public and private spheres. A cyber attack against a government agency or a defense contractor is an attack against our nation. But so is an attack on a private company that provides power or clean water to millions of Americans. An attack against a privately owned and operated piece of our nation's critical infrastructure is an attack on all of us.

Since I have been working on this issue, I've had a lot of good, productive discussions with leaders in our business community, our military, and in other government agencies who understand this threat and have good ideas about how we can tackle it. But we've also wasted a lot of time, by turning an urgent national security issue into a partisan political fight. Back in 2010, we passed a cyber bill out of the Commerce Committee unanimously, without a vote. By the fall of 2012, we couldn't even get enough votes to close debate on the Senate floor, even though our country's top national security leaders were urging us to act.

The Obama Administration got tired of waiting for us. I can't blame them. This is a problem that is growing worse every day. On February 12, 2013, President Obama released an Executive order that takes some very important steps to start dealing with our cybersecurity problems. The order marshals the resources and the expertise we have in many different Federal agencies to start strengthening our country's ability to defend ourselves from cyber attacks.

The Obama Administration worked very hard to make this Executive order a welcoming invitation to the private sector to work together on this problem. It seeks to formalize and strengthen the working relationships many companies already have with our cybersecurity experts in the Federal Government. One of the most important initiatives in the Executive order is to start a process at the National Institute of Standards and Technology (NIST) that will develop cybersecurity standards and best practices with U.S. companies.

We are going to hear more about the Executive order from our witnesses today, and we are going hear a lot more about cybersecurity in the 113th Congress. The Senators sitting at this dais today—and many more who are not sitting up here—understand what an urgent issue this is. We understand that some of steps we need to take to defend our people and our critical infrastructure cannot be accomplished

by a presidential order. We have to work with each other. We have to trust each other. We have to move forward.

And I turn to my distinguished Chairman.

And the only—I regret to say this, but this is—since it's not a public meeting, it doesn't hurt me anymore—the only West Virginian—no——

Senator CARPER. One of two.

Chairman ROCKEFELLER.—one of two in the United States Senate. The one who isn't is the one who's just finished talking.

STATEMENT OF HON. THOMAS R. CARPER,
U.S. SENATOR FROM DELAWARE

Chairman CARPER. And the one who is wishes he had his money.

[Laughter.]

Chairman CARPER. Nothing like being born in a log cabin, I'll tell you.

I'm thrilled to be here with Senator Rockefeller, our Chair—co-Chair—and Senator Thune and my wingman, here, Tom Coburn, with whom I've worked on a lot of things.

I'm delighted with our witnesses.

And, Secretary, Pat, we're happy that you could join us today.

I'm told that our committees have not held a joint hearing for over 35 years; I guess, since 1975, to be exact. We need to be able to work together; this is a shared responsibility, and not just between government and private sector; this is a shared responsibility here on Capitol Hill: executive branch, legislative branch, and different committees, and different parties. So, this is a great way to get started. I'm happy that we're doing this.

But, we're having this hearing today because, as Chairman Rockefeller has said, America's economy and our national security are under attack. This is not the kind of war that some of us served in earlier in our lives or read about in the history books or have watched on television. The war that's occurring today is a war that's occurring in cyberspace, it's occurring in realtime, because, literally as I speak, sophisticated cyber thieves are stealing our ideas, our intellectual property, the very innovation, or the seed corn, if you will, that fuels our economy in years to come.

Recent report by Mandiant, an American cybersecurity firm, points the finger for much—not all, but much of the cyber threat thievery that's going on, to a military unit in China. Even more alarming are the reports that hackers are constantly probing the companies that run our nation's critical infrastructure—our electric grid, our gas lines, our waterworks, the banking systems, among others.

Since this past summer, for example, websites for a number of major U.S. banks have become the target of repeated cyber attacks that have caused a disruption and service delays. We read about that every week, almost every day. But, once inside a company network, these hackers can do a lot more than steal information or create a temporary nuisance. Among other things, they can shut down our electric grid or release dangerous chemicals into our water supply or into our air. We only have to think about the cyber attack that reportedly destroyed more than 30,000 computers at oil

giant Saudi Aramco to know that the threat is real and it is serious.

Several of our colleagues, including Senator Rockefeller, Senators Feinstein and Collins, and former Chair of the Committee that I'm now privileged to chair, Joe Lieberman, worked diligently with others to move cybersecurity legislation that Senator Rockefeller has mentioned. Unfortunately, we couldn't come together to pass this vital piece of bipartisan legislation. But, given the growing cyber threats that America faces, we're now more determined than ever to put in place a thoughtful, comprehensive cyber policy to protect our nation, its people, its critical infrastructures, and its economy.

Because of Congress's failure to act last year, and the serious nature of the threat, the President has issued, as we know, an Executive order, last month, to better protect our nation's cyber networks. Instead of drafting the order behind closed doors, the White House was very open with the process, conducting numerous listening sessions with companies and trade groups so that the good ideas could be freely shared and adopted, and bad ideas could be rejected.

Final product is an order that takes a number of critical steps to improve the security of our critical infrastructure.

One of these steps enhances the way we share cyber threat information between the Federal Government and the private sector. For instance, in response to the concerns of many in industry, the order looks to increase the volume, the timeliness, and the quantity of cyber threat information shared with the private sector. The order also relies on public-private partnerships to strengthen the digital backbone of our most sensitive systems. In fact, the order calls on the private sector to lead the development of new security framework, in coordination with NIST, National Institution—National Institute of Standards and Technology.

Companies may voluntarily adopt the new cybersecurity framework or work with their current regulations on their solutions. To encourage the adoption of any new framework, though, the order calls for using carrots instead of sticks. For example, the order requires the Department of Homeland Security and other Federal agencies to establish a set of incentives to promote participation in the program. It also requires Homeland Security to expedite the granting of security clearances to the people who run our critical infrastructure, so that industry can better understand the threats that they face.

Privacy and civil liberties protections are also a key consideration throughout the order. In fact, agencies are required to incorporate privacy safeguards in all their activities under the order. And, while I commend the President for issuing this important order, there's only so much that he, or any President, could do, using the authorities granted to a President under existing law. Those authorities are simply not enough to get the job done. That's where we come in.

Now is the time to begin the process of gathering input from the administration and the broad array of stakeholders in order to ascertain what Congress needs to do, what we need to do, to build on, or fill in the gaps, if you will, around this Executive order so that—that the President has promulgated.

For example, we know that what—that more needs to be done on information sharing so that companies can more freely share their best practices and threat information with each other and with our government. We should also consider how we can further improve the protection of our nation's critical infrastructure, including offering incentives, such as liability protection, in certain instances.

In addition, we need to be modernize the dated process we have in place to ensure that the security of our Federal network, something that we call FISMA, an area that Senator Coburn and I have worked on for quite some time, along with Senator Collins.

It's also important for us to clarify the roles and responsibilities of Federal agencies involved in cybersecurity so that we know who should be held accountable for our successes or failures in tackling this growing threat.

And finally, we must also continue to develop the next generation of cyber professionals, grow our own, and better coordinate our cyber research-and-development efforts. A lot of people in this country of ours question, today, whether we're still able to set aside partisan differences or other differences—the stakes are high—and summon the political will to do what's best for America. The stakes are high. And it's important—as the Chairman has said, here—important that we should set aside our difference, whether political or otherwise, and do what's right for our country. And I'm confident, I'm encouraged, that, with the cooperation of the folks that are on these committees and our colleagues with whom we serve, that we're up to the task, and we're going to seize this opportunity.

Thank you, Mr. Chairman.

[The prepared statement of Chairman Carper follows:]

PREPARED STATEMENT OF HON. THOMAS R. CARPER, U.S. SENATOR FROM DELAWARE

I am very pleased to be here today with our colleagues from the Senate Commerce Committee hosting a joint hearing on cybersecurity, an incredibly important topic for our country. I would like to thank Chairman Rockefeller, Ranking Member Thune, and my Ranking Member, Dr. Coburn—along with our staff members—for all their work on this hearing. I would also like to thank our witnesses for being here today and for their valuable service to our country.

I am told that our Committees have not held a joint hearing for over 35 years—since 1975 to be exact. It is fitting that we have come together again to address this issue because we definitely need a true partnership to pass comprehensive cybersecurity legislation in this Congress—a partnership between Democrats and Republicans, the House and the Senate, Congress and the Administration; and, as the title of this hearing indicates, between government and industry.

We are having this hearing today because America's economy and our national security are under attack. This is not the kind of war that some of us served in earlier in our lives, or read about in history books, or watched on TV. This war is occurring in cyberspace and in real time. Literally as I speak, sophisticated cyber thieves are stealing American ideas and intellectual property—the very innovation that fuels our economy.

A recent report by Mandiant, an American cybersecurity firm, points the finger for much of this cyber theft to a military unit in China. Even more alarming are the reports that hackers are constantly probing the companies that run our Nation's critical infrastructure—our electrical power grid, gas lines, waterworks, and banking system, among others.

Since this past summer, for example, websites for a number of major U.S. banks have become the target of repeated cyber attacks that have caused disruption and service delays. But once inside a company network, these hackers can do a lot more than steal information or create a temporary nuisance. Among other things, they can shut down our electric grid or release dangerous chemicals into our water supply.

We only have to think about the cyber attack that reportedly destroyed more than 30,000 computers at oil giant Saudi Aramco to know this threat is real—and serious. Several of our colleagues, including Senators Rockefeller, Feinstein, and Collins, and the former Chairman of the Committee I now chair, Joe Lieberman, worked diligently to move cyber legislation last year. Unfortunately, the Senate could not come together to pass this vital piece of bipartisan legislation. But given the growing cyber threats that America faces, we are now more determined than ever to put in place a comprehensive cyber policy to protect our nation, its people, its critical infrastructure, and its economy.

Because of Congress' failure to act last year and the serious nature of the threat, the President issued an Executive Order last month to better protect our Nation's cyber networks. Instead of drafting the Order behind closed doors, the White House was very open with the process, conducting numerous "listening sessions," with companies and trade groups so that good ideas could be freely shared and adopted. The final product is an Order that takes a number of critical steps to improve the security of our critical infrastructure.

One of these steps enhances the way we share cyber threat information between the Federal Government and the private sector. For instance, in response to the concerns of many in industry, the Order looks to increase the volume, timeliness, and quality of cyber threat information shared with the private sector.

The Order also relies on a public-private partnership to strengthen the digital backbone of our most sensitive systems. In fact, the Order calls on the private sector to lead the development of new security frameworks in coordination with the National Institute of Standards and Technology.

Companies may voluntarily adopt the new cybersecurity framework or work with their current regulators on other solutions. To encourage the adoption of any new framework, the Order calls for using carrots instead of sticks. For example, the Order requires the Department of Homeland Security and other Federal agencies to establish a set of incentives to promote participation in the program.

It also requires Homeland Security to expedite the granting of security clearances to the people who run our critical infrastructure, so that industry can better understand the threats they face. Privacy and civil liberties protections are also a key consideration throughout the Order. In fact, agencies are required to incorporate privacy safeguards in all their activities under the Order.

While I commend the President for issuing this very important Order, there was only so much he could do using the authorities granted to him under existing law. Those authorities are simply not enough to get the job done. Now is the time to begin the process of gathering input from the Administration and a broad array of stakeholders in order to ascertain what Congress needs to do to build on the Executive order that the President has promulgated.

For example, we know that more needs to be done on information sharing so that companies can more freely share best practices and threat information with each other, and with the Federal Government. We should also consider how we can further improve the protection of our Nation's critical infrastructure, including offering incentives such as liability protection in certain instances. In addition, we need to modernize the dated process we have in place to ensure the security of our Federal networks. This is an area that I have worked on for years.

It is also important for us to clarify the roles and responsibilities of Federal agencies involved in cybersecurity so that we know who should be held accountable for our success or failure in tackling this growing threat. Finally, we must also continue to develop the next generation of cyber professionals and better coordinate our cyber research and development efforts.

A lot of people in this country of ours question today whether we're still able to set aside our partisan differences when the stakes are high and summon the political will to do what's best for America. I believe this joint hearing is a good step in showing the American people we can. I look forward to working with our colleagues, as well as with the Administration, industry, and other stakeholders, to pass critically needed cyber legislation.

Chairman ROCKEFELLER. The distinguished Ranking Member of the Commerce Committee, Senator Thune.

STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. Thank you, Mr. Chairman and Chairman Carper. I look forward, along with you and with Senator Coburn and

members of both of our committees, to examining the need for a greater cybersecurity partnership between the private sector and the Federal Government.

No one can deny the serious threat that we're confronting in cyberspace. Almost daily, we learn of new cyber threats and attacks targeting our government agencies and companies that drive our economy. In these perilous economic times, it's especially troubling that the intellectual capital that fuels our prosperity is being siphoned off by cyber criminals and even nation—states.

The National Counterintelligence Executive, the country's chief counterintelligence official, summed it up this way in 2011, and I quote, "Trade secrets developed over thousands of working hours by our brightest minds are stolen in a split second and transferred to our competitors." This large-scale theft cannot be allowed to continue unchecked. We must find solutions that leverage the innovation and know-how of the private sector, as well as the expertise and information held by the Federal Government. And, given the escalating nature of the threat, we should look for solutions that will have an immediate impact.

As today's hearing title suggests, one thing we must do is strengthen the partnership between the government and the private sector. As one of our witnesses, David Kepler, of The Dow Chemical Company, observed in his testimony, timely information sharing between government and industry, and among industry peers, is key to this collaboration.

The Chair of the House Intelligence Committee has said that, according to intelligence officials, allowing the government to share classified information with private companies could stop up to 90 percent of cyber attacks on U.S. networks. Even if the figure was only 60 to 70 percent, the return would be well worth the effort.

Improving research and development is another area where our focus could yield new tools to secure the cyber domain. We should not underestimate the value of R&D. I'm proud to know that South Dakota's own Dakota State University is one of only four schools in the nation designated by the National Security Agency as a National Center of Academic Excellence in Cyber Operations.

It's no secret that, during the last Congress, the Senate reached an impasse on cybersecurity legislation. It is my hope—and I suspect that it's our shared hope—that we can avoid another stalemate in this Congress. Today's hearing represents a good start.

As we all recognize, this issue crosses the jurisdictional boundaries of many committees, so it is appropriate, if somewhat challenging, that we've joined with our colleagues on the Homeland Security and Governmental Affairs Committee today. Of course, given the importance of this topic and the value of hearing from multiple stakeholders, I look forward to additional sessions in the Commerce Committee as we seek consensus on this vital matter.

Our hearing today takes place against the backdrop of the President's recently released Executive order on cybersecurity and related Presidential policy directive. Even though I, like many of my colleagues, was skeptical about executive action, the order's release may provide an opportunity for Congress to find common ground on other steps that will improve our cybersecurity. Of course, we

must also conduct meaningful oversight of the Executive order's implementation.

I look forward to hearing from Secretary Napolitano and Under Secretary Gallagher today regarding the steps the Department of Homeland Security and the National Institute of Standards and Technology are taking to ensure that the Executive order's promise of improved partnership and collaboration with the private sector is realized in practice. I'm particularly interested in hearing about how the Executive order builds upon or enhances existing mechanism for public-private collaboration. And I'll be interested in the views of our GAO witness, Greg Wilshusen, as to whether the Federal Government is up to the task envisioned by the Executive order, given persistent shortcomings in its own cybersecurity efforts identified by the watchdog agency.

Again, Mr. Chairman, I thank you, and I thank all of the witnesses for being here today, and I look forward to hearing their testimony.

Chairman ROCKEFELLER. Distinguished Senator from Oklahoma, Tom Coburn.

STATEMENT OF HON. TOM COBURN,
U.S. SENATOR FROM OKLAHOMA

Senator COBURN. Thank you, Mr. Chairman.

Welcome, to all the witnesses. I appreciate you being here.

Senator Carper and I had a little demonstration or presentation on the Executive order yesterday, and I have to say I was impressed with the thoroughness and the presentation of it.

I'm highly disappointed that OMB didn't release the FISMA report. And there's no reason for it, other than it's—shows significant criticism of our ability to manage critical information within the Federal Government. And I will apologize to them vociferously if, in fact—my assessment of that report. But, to not put it out before this hearing is absolutely ridiculous, because we all know—and the GAO's going to testify today what we all know—is the status within our own government on how well we're doing. And so, it's unfortunate that we've chosen not to have a critical piece of information that analyzes a report card on us for this hearing.

The—I am appreciative of the leadership of the President and his staff in doing this Executive order. I think it was timely and it was appropriate. And I'll speak to the issue that nobody wants to directly speak to, is—the reason the bill didn't go through the Senate is because there's a—there is a disagreement on the liability protections for business and industry, when they share their information, to protect them against frivolous lawsuits. And in the hearings that Senator Carper and I have had that have been classified thus far, there hasn't been one person who's testified—all administrative witnesses, all administration—who don't agree that those protections are going to have to be there for us to accomplish what we need to do for our country. And so, what we have to do is, we have to get past that one issue, and we have to address the real issues in front of us.

The other thing that I would like to emphasize is the fact—and Senator Thune spoke about it, and I know Senator Rockefeller and Senator Carper care immensely about it—and that's the intellec-

tual property loss that this country loses every year. And General Alexander, head of the NSA, has said it's around $400 billion a year. And if we do not create a workable situation, what we're doing is taking the investment that we spend every year, that we want to spend, in terms of RD in this country, and giving it away.

So, we have to find a way to solve this problem, in the Senate, and we have to work across the aisle and across the special interest groups that don't want certain things because it might create a lack of a supreme benefit for their cause. What we have to do is what's in the best interests of the nation. And I think the President has shown real leadership with this Executive order, and now we need to come behind it and firm it up.

And I appreciate, also, Senator Rockefeller, his cooperation on the witnesses for this. I want to thank you publicly for that. Having a hearing on cybersecurity and not listening to the expert at GAO would be inappropriate. And Mr. Wilshusen is here, and he's knowledgeable, and I look forward to his testimony, on the second panel.

Thank you.

[The prepared statement of Ranking Member Coburn follows:]

PREPARED STATEMENT OF HON. TOM COBURN, U.S. SENATOR FROM OKLAHOMA, RANKING MEMBER, U.S. SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Thank you, Mr. Chairman. Welcome to all the witnesses. I appreciate you being here. Senator Carper and I had a little demonstration or presentation on the executive order yesterday. And I have to say I was impressed with the thoroughness and the presentation of it.

I am highly disappointed that OMB didn't release the FISMA report. There is no reason for it other than it shows significant criticism of our ability to manage critical information within the Federal Government. I will apologize to them vociferously if, in fact, my assessment of that report—but to not put it out before this hearing is absolutely ridiculous, because we all know, and the GAO's going to testify today what we all know, is the status within our own government on how well we're doing, and so it's unfortunate that we have chosen not to have a critical piece of information that analyzes a report card on us for this hearing.

I am appreciative of the leadership of the President and his staff in doing this Executive order. I think it was timely and appropriate. I'll speak to the issue that nobody wants directly to speak to, is the reason the bill didn't go through the Senate is because there is a disagreement on the liability protections for business and industry when they share their information to protect them against frivolous lawsuits. In the hearings that Senator Carper and I have had, that have been classified thus far, there hadn't been one person who has testified, all the administrative witnesses—all of administration—who do not agree that those protections are going to have to be there for us to accomplish what we need to do for our country. We have to get past that one issue, and we have to address the issues in front of us.

The other thing that I would like to emphasize is the intellectual property loss that this country loses every year. General Alexander, head of the NSA, has said it's around $400 billion a year, and if we do not create a workable situation, what we are doing is taking the investment that we spend every year that we want to spend in terms of R&D in this country, and giving it away.

We have to find a way to solve this problem in the Senate, and we have to work across the aisle and across the special interest groups that don't want certain things, because it might create a lack of a supreme benefit for their cause. What we have to do is what's in the best interest of the nation, and I think the President has shown real leadership with this Executive order, and now we need to come behind and firm it up.

I appreciate—also, Senator Rockefeller, his cooperation on the witnesses for this. I want to thank you publicly for that. Having a hearing on cybersecurity and not listening to the expert at GAO would be inappropriate, and Mr. Wilshusen is here, and he's knowledgeable, and I look forward to his testimony in the second panel.

Thank you.

Chairman ROCKEFELLER. Thank you, Senator Coburn.

And we now go to our first two witnesses. We're glad they're here.

The Honorable Janet Napolitano, who's Secretary, U.S. Department of Homeland Security.

I see you at more hearings, on more television, than anybody else within a 10-mile radius of Washington, D.C. But, fortunately, you're here today for us. Please proceed.

STATEMENT OF HON. JANET NAPOLITANO, SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary NAPOLITANO. Well, thank you. Thank you, Chairman Rockefeller and Ranking Member Thune and Chairman Carper, Ranking Member Coburn, members of the Committee. I appreciate the opportunity to testify regarding our cybersecurity efforts at the Department of Homeland Security. And I also want to thank Under Secretary Gallagher for our partnership with NIST with the Department of Commerce.

This is, as you all have acknowledged, an urgent and important topic. As you know, DHS is responsible for securing unclassified Federal civilian government networks and working with owners and operators of critical infrastructure to help them secure their own networks. We also coordinate the national response to significant cyber incidents, and create and maintain a common operational picture for cyberspace across the government.

This is critical, time-sensitive work, because we confront a dangerous combination of known and unknown cyber vulnerabilities and adversaries with strong and rapidly expanding capabilities. Threats range from denial-of-service attacks to theft of valuable intellectual property to intrusions against government networks and systems that control our nation's critical infrastructure. These attacks come from every part of the globe. They come every minute of every day. They are continually increasing in seriousness and sophistication.

To protect Federal networks, DHS is deploying technology to detect and to block cyber intrusions, and we are developing continuous diagnostic capabilities while providing guidance on what agencies need to do to protect themselves. We also work closely and regularly with owners and operators of critical infrastructure to strengthen their facilities through onsite risk assessment, mitigation, and incident response, and by sharing risk and threat information. For example, we provided classified cyber threat briefings and technical assistance to help banks improve their defensive capabilities following the recent spate of DDOS attacks.

DHS is home to the National Cybersecurity and Communications Integration Center, the NCCIC. The NCCIC is an around-the-clock cyber situational awareness and incident-response center, which, over the past 4 years—and that's as old as it is—has responded to nearly a half a million incident reports and released more than 26,000 actionable cybersecurity alerts to public-and private-sector partners. Last year, the Computer Emergency Readiness Team, US-CERT, resolved approximately 190,000 cyber incidents and issued more than 7,450 alerts—in and of itself, a 68 percent increase from the year before—and our Industrial Control System

Cyber Emergency Response Team responded to 177 incidents while completing 89 site visits, deploying 15 teams to respond to significant private-sector cyber incidents involving control systems.

Since 2009, DHS components have prevented $10 billion in potential losses through cyber crime investigations. We have arrested more than 5,000 individuals in connection with cyber crime. And we partner closely with the Departments of Justice and Defense to ensure that a call to one is a call to all. So, while each agency operates within the parameters of its authorities, our overall Federal response to cyber incidents of consequence is coordinated among the three agencies. Where agency authorities overlap, as in law enforcement protection and response, we also directly coordinate with and support each other.

This synchronization—a call to one is a call to all—ensures that all of our capabilities are brought to bear against cyber threats, enhances our ability to share timely and actionable information with a variety of partners.

But, while our accomplishments are significant and cybersecurity remains a priority for the administration, in order to be able to best meet this growing threat, we need Congress to enact a suite of comprehensive cybersecurity legislation. I appreciate the efforts made in the last Congress to pass bipartisan legislation, but the inability to get this done has, indeed, required the President to take executive action.

The EO [Executive order] on Improving Critical Infrastructure Cybersecurity supports more efficient sharing of realtime cyber threat information with the private sector. It directs DHS to develop a voluntary program to promote the adoption of a new cybersecurity framework, and assists the private sector in its implementation. The accompanying Presidential Policy Directive on Critical Infrastructure, Security, and Resilience also directs the executive branch to strengthen our capability to understand and share information about how well critical infrastructure systems are functioning, and the consequence of potential failure. And it calls for a comprehensive research-and-development plan to guide the government's effort to enhance market-based innovation.

These two documents, the EO and the PPD, reflect input from stakeholders of all viewpoints across government, industry, and the advocacy community. Their ideas and lessons were incorporated, as were rigorous protections for individual privacy and civil liberties. Importantly, the EO calls us to work within current authorities and increase voluntary cooperation with the private sector. It does not grant any new regulatory authority or establish additional incentives for participation in a voluntary program.

Nonetheless, we continue to believe that a comprehensive suite of legislation is necessary to build stronger, more effective public/private partnerships in the realm of cyber. Specifically, Congress should enact legislation to incorporate privacy and civil liberty safeguards into all aspects of cybersecurity, further increase information sharing, and establish and promote the adoption of standards for critical infrastructure, give law enforcement additional tools to fight crime in the Digital Age, create a national data-breach reporting requirement; and, finally, give DHS hiring authority equivalent to that of the NSA.

We also know that threats to cyberspace, and the need to address them, do not diminish because of budget cuts. Even in the current fiscal climate, we do not have the luxury of making significant reductions to our capabilities without having significant impacts. Sequester reductions will require us to scale back the development of critical capabilities for the defense of Federal cyber networks. It will disrupt long-term efforts to grow our cybersecurity workforce, and delay the implementation of E3A by approximately 1 year. In addition, sequester has resulted in canceling major cybersecurity exercises by which, involving international, Federal, State, local, private-sector partners, we actually work through the various problem sets and scenarios we confront.

The American people expect us to secure the country from a growing cyber threat and to ensure that critical infrastructure is protected. Further action is needed by Congress, including immediate action to address the sequester, if we are to meet our responsibilities. We must act now, not years from now.

So, I look forward to working with both committees to make sure we continue to do everything possible to keep the nation safe.

I thank you for your continued guidance and support, and for the opportunity to be with you this afternoon.

[The prepared statement of Secretary Napolitano follows:]

PREPARED STATEMENT OF HON. JANET NAPOLITANO, SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Chairmen Rockefeller and Carper, Ranking Members Thune and Coburn, and Members of the Committees:

I am pleased to join you today, and I thank the Committee for your strong support for the Department of Homeland Security (DHS) over the past four years and, indeed, since the Department's founding ten years ago.

I can think of no more urgent and important topic in today's interconnected world than cybersecurity, and I appreciate the opportunity to explain the Department's mission in this space and how we continue to improve cybersecurity for the American people as well as work to safeguard the nation's critical infrastructure and protect the Federal Government's networks.

Current Threat Landscape

Cyberspace is woven into the fabric of our daily lives. According to recent estimates, this global network of networks encompasses more than two billion people with at least 12 billion computers and devices, including global positioning systems, mobile phones, satellites, data routers, ordinary desktop computers, and industrial control computers that run power plants, water systems, and more.

While this increased connectivity has led to significant transformations and advances across our country—and around the world—it also has increased the importance and complexity of our shared risk. Our daily life, economic vitality, and national security depend on cyberspace. A vast array of interdependent IT networks, systems, services, and resources are critical to communication, travel, powering our homes, running our economy, and obtaining government services. No country, industry, community or individual is immune to cyber risks. The word "cybersecurity" itself encompasses protection against a broad range of malicious activity, from denial of service attacks, to theft of valuable trade secrets, to intrusions against government networks and systems that control our critical infrastructure.

The United States confronts a dangerous combination of known and unknown vulnerabilities in cyberspace and strong and rapidly expanding adversary capabilities. Cyber crime has also increased significantly over the last decade. Sensitive information is routinely stolen from both government and private sector networks, undermining the integrity of the data contained within these systems. We currently see malicious cyber activity from foreign nations engaged in espionage and information warfare, terrorists, organized crime, and insiders. Their methods range from distributed denial of service (DDoS) attacks and social engineering to viruses and

other malware introduced through thumb drives, supply chain exploitation, and leveraging trusted insiders' access.

We have seen motivations for attacks vary from espionage by foreign intelligence services to criminals seeking financial gain and hackers who may seek bragging rights in the hacker community. Industrial control systems are also targeted by a variety of malicious actors who are usually intent on damaging equipment and facilities or stealing data. Foreign actors are also targeting intellectual property with the goal of stealing trade secrets or other sensitive corporate data from U.S. companies in order to gain an unfair competitive advantage in the global market.

Cyber attacks and intrusions can have very real consequences in the physical world. Last year, DHS identified a campaign of cyber intrusions targeting natural gas and pipeline companies that was highly targeted, tightly focused and well crafted. Stolen information could provide an attacker with sensitive knowledge about industrial control systems, including information that could allow for unauthorized operation of the systems. As the President has said, we know that our adversaries are seeking to sabotage our power grid, our financial institutions, and our air traffic control systems. These intrusions and attacks are coming all the time and they are coming from different sources and take different forms, all the while increasing in seriousness and sophistication.

The U.S. Government has worked closely with the private sector during the recent series of denial-of-service incidents. We have provided classified cyber threat briefings and technical assistance to help banks improve their defensive capabilities and we have increased sharing and coordination among the various government elements in this area. These developments reinforce the need for government, industry, and individuals to reduce the ability for malicious actors to establish and maintain capabilities to carry out such efforts.

In addition to these sophisticated attacks and intrusions, we also face a range of traditional crimes that are now perpetrated through cyber networks. These include child pornography and exploitation, as well as banking and financial fraud, all of which pose severe economic and human consequences. For example, in March 2012, the U.S. Secret Service (USSS) worked with U.S. Immigration and Customs Enforcement (ICE) to arrest nearly 20 individuals in its "Operation Open Market," which seeks to combat transnational organized crime, including the buying and selling of stolen personal and financial information through online forums. As Americans become more reliant on modern technology, we also become more vulnerable to cyber exploits such as corporate security breaches, social media fraud, and spear phishing, which targets employees through e-mails that appear to be from colleagues within their own organizations, allowing cyber criminals to steal information.

Cybersecurity is a shared responsibility, and each of us has a role to play. Emerging cyber threats require the engagement of our entire society—from government and law enforcement to the private sector and, most importantly, members of the public. The key question, then, is how do we address this problem? This is not an easy question because cybersecurity requires a layered approach. The success of our efforts to reduce cybersecurity risks depends on effective identification of cyber threats and vulnerabilities, analysis, and enhanced information sharing between departments and agencies from all levels of government, the private sector, international entities, and the American public.

Roles, Responsibilities, Activities

DHS is committed to ensuring cyberspace is supported by a secure and resilient infrastructure that enables open communication, innovation, and prosperity while protecting privacy, confidentiality, and civil rights and civil liberties by design.

Securing Federal Civilian Government Networks

DHS has operational responsibilities for securing unclassified Federal civilian government networks and working with owners and operators of critical infrastructure to secure their networks through cyber threat analysis, risk assessment, mitigation, and incident response capabilities. We also are responsible for coordinating the national response to significant cyber incidents and for creating and maintaining a common operational picture for cyberspace across the government.

DHS directly supports Federal civilian departments and agencies in developing capabilities that will improve their cybersecurity posture in accordance with the Federal Information Security Management Act (FISMA). To protect Federal civilian agency networks, our National Protection and Programs Directorate (NPPD) is deploying technology to detect and block intrusions through the National Cybersecurity Protection System and its EINSTEIN protective capabilities, while providing

guidance on what agencies need to do to protect themselves and measuring implementation of those efforts.

NPPD is also developing a Continuous Monitoring as a Service capability, which will result in an array of sensors that feed data about an agency's cybersecurity risk and present those risks in an automated and continuously-updated dashboard visible to technical workers and managers to enhance agencies' ability to see and counteract day-to-day cyber threats. This capability will support compliance with Administration policy, be consistent with guidelines set forth by the National Institute of Standards and Technology (NIST), and enable Federal agencies to move from compliance-driven risk management to data-driven risk management. These activities will provide organizations with information necessary to support risk response decisions, security status information, and ongoing insight into effectiveness of security controls.

Protecting Critical Infrastructure

Critical infrastructure is the backbone of our country's national and economic security. It includes power plants, chemical facilities, communications networks, bridges, highways, and stadiums, as well as the Federal buildings where millions of Americans work and visit each day. DHS coordinates the national protection, prevention, mitigation, and recovery from cyber incidents and works regularly with business owners and operators to take steps to strengthen their facilities and communities. The Department also conducts onsite risk assessments of critical infrastructure and shares risk and threat information with state, local and private sector partners.

Protecting critical infrastructure against growing and evolving cyber threats requires a layered approach. DHS actively collaborates with public and private sector partners every day to improve the security and resilience of critical infrastructure while responding to and mitigating the impacts of attempted disruptions to the Nation's critical cyber and communications networks and to reduce adverse impacts on critical network systems.

DHS enhances situational awareness among stakeholders, including those at the state and local level, as well as industrial control system owners and operators, by providing critical cyber threat, vulnerability, and mitigation data, including through Information Sharing and Analysis Centers, which are cybersecurity resources for critical infrastructure sectors. DHS is also home to the National Cybersecurity & Communications Integration Center (NCCIC), a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

Responding to Cyber Threats

DHS is responsible for coordinating the Federal Government response to significant cyber or physical incidents affecting critical infrastructure. Since 2009, the NCCIC has responded to nearly half a million incident reports and released more than 26,000 actionable cybersecurity alerts to our public and private sector partners. The DHS Office of Intelligence and Analysis is a key partner in NCCIC activities, providing tailored all-source cyber threat intelligence and warning to NCCIC components and public and private critical infrastructure stakeholders to prioritize risk analysis and mitigation.

An integral player within the NCCIC, the U.S. Computer Emergency Readiness Team (US–CERT) also provides response support and defense against cyber attacks for Federal civilian agency networks as well as private sector partners upon request. US–CERT collaborates and shares information with state and local government, industry, and international partners, consistent with rigorous privacy, confidentiality, and civil liberties guidelines, to address cyber threats and develop effective security responses. In 2012, US–CERT processed approximately 190,000 cyber incidents involving Federal agencies, critical infrastructure, and our industry partners. This represents a 68 percent increase from 2011. In addition, US–CERT issued over 7,455 actionable cyber-alerts in 2012 that were used by private sector and government agencies to protect their systems, and had over 6,400 partners subscribe to the US–CERT portal to engage in information sharing and receive cyber threat warning information.

The Department's Industrial Control Systems Cyber Emergency Response Team (ICS–CERT) also responded to 177 incidents last year while completing 89 site assistance visits and deploying 15 teams with US–CERT to respond to significant private sector cyber incidents. DHS also empowers owners and operators through a cyber self-evaluation tool, which was used by over 1,000 companies last year, as well as in-person and on-line training sessions.

Successful response to dynamic cyber threats requires leveraging homeland security, law enforcement, and military authorities and capabilities, which respectively promote domestic preparedness, criminal deterrence and investigation, and national defense. DHS, the Department of Justice (DOJ), and the Department of Defense (DOD) each play a key role in responding to cybersecurity incidents that pose a risk to the United States. In addition to the aforementioned responsibilities of our Department, DOJ is the lead Federal department responsible for the investigation, attribution, disruption, and prosecution of domestic cybersecurity incidents while DOD is responsible for securing national security and military systems as well as gathering foreign cyber threat information and defending the Nation from attacks in cyberspace. DHS supports our partners in many ways. For example, the United States Coast Guard as an Armed Force has partnered with U.S. Cyber Command and U.S. Strategic Command to conduct military cyberspace operations.

While each agency operates within the parameters of its authorities, the U.S. Government's response to cyber incidents of consequence is coordinated among these three agencies such that "a call to one is a call to all." Synchronization among DHS, DOJ, and DOD not only ensures that whole of government capabilities are brought to bear against cyber threats, but also improves government's ability to share timely and actionable cybersecurity information among a variety of partners, including the private sector.

Combating Cybercrime

DHS employs more law enforcement agents than any other Department in the Federal Government and has personnel stationed in every state and in more than 75 countries around the world. To combat cyber crime, DHS relies upon the skills and resources of the USSS and ICE and works in cooperation with partner organizations to investigate cyber criminals. Since 2009, DHS has prevented $10 billion in potential losses through cyber crime investigations and arrested more than 5,000 individuals for their participation in cyber crime activities.

The Department leverages the 31 USSS Electronic Crimes Task Forces (ECTF), which combine the resources of academia, the private sector, and local, state and Federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructure. A recently executed partnership between ICE Homeland Security Investigations and USSS demonstrates the Department's commitment to leveraging capability and finding efficiencies. Both organizations will expand participation in the existing ECTFs. In addition to strengthening each agency's cyber investigative capabilities, this partnership will produce benefits with respect to the procurement of computer forensic hardware, software licensing, and training that each agency requires. The Department is also a partner in the National Cyber Investigative Joint Task Force, which serves as a collaborative entity that fosters information sharing across the interagency.

We work with a variety of international partners to combat cybercrime. For example, through the U.S.-EU Working Group on Cybersecurity and Cybercrime, which was established in 2010, we develop collaborative approaches to a wide range of cybersecurity and cybercrime issues. In 2011, DHS participated in the Cyber Atlantic tabletop exercise, a U.S.-EU effort to enhance international collaboration of incident management and response, and in 2012, DHS and the EU signed a joint statement that advances transatlantic efforts to enhance online safety for children. ICE also works with international partners to seize and destroy counterfeit goods and disrupt websites that sell these goods. Since 2010, ICE and its partners have seized over 2,000 domain names associated with businesses selling counterfeit goods over the Internet. To further these efforts, the Administration issued its Strategy on Mitigating the Theft of U.S. Trade Secrets last month. DHS will act vigorously to support the Strategy's efforts to combat the theft of U.S. trade secrets—especially in cases where trade secrets are targeted through illicit cyber activity by criminal hackers.

In addition, the National Computer Forensic Institute has trained more than 1,000 state and local law enforcement officers since 2009 to conduct network intrusion and electronic crimes investigations and forensic functions. Several hundred prosecutors and judges as well as representatives from the private sector have also received training on the impact of network intrusion incident response, electronic crimes investigations, and computer forensics examinations.

Building Partnerships

DHS serves as the focal point for the Government's cybersecurity outreach and awareness efforts. Raising the cyber education and awareness of the general public creates a more secure environment in which the private or financial information of individuals is better protected. For example, the Multi-State Information Sharing

and Analysis Center (MS–ISAC) opened its Cyber Security Operations Center in November 2010, which has enhanced NCCIC situational awareness at the state and local government level and allows the Federal Government to quickly and efficiently provide critical cyber threat, risk, vulnerability, and mitigation data to state and local governments. MS–ISAC has since grown to include all 50 states, three U.S. territories, the District of Columbia, and more than 200 local governments.

The Department also has established close working relationships with industry through partnerships like the Protected Critical Infrastructure Information (PCII) Program, which enhances voluntary information sharing between infrastructure owners and operators and the government. The Cyber Information Sharing and Collaboration Program established a systematic approach to cyber threat information sharing and collaboration between critical infrastructure owners and operators across the various sectors. And, in 2010, we launched a national campaign called *Stop.Think.Connect* to spread public awareness about how to keep our cyber networks safe.

In addition, DHS works closely with international partners to enhance information sharing, increase situational awareness, improve incident response capabilities, and coordinate strategic policy issues in support of the Administration's *International Strategy for Cyberspace.* For example, the Department has fostered international partnerships in support of capacity building for cybersecurity through agreements with Computer Emergency Response and Readiness Teams as well as the DHS Science & Technology Directorate (S&T). Since 2009, DHS has established partnerships with Australia, Canada, Egypt, India, Israel, the Netherlands, and Sweden.

Fostering Innovation

The Federal Government relies on a variety of stakeholders to pursue effective research and development projects that address increasingly sophisticated cyber threats. This includes research and development activities by the academic and scientific communities to develop capabilities that protect citizens by enhancing the resilience, security, integrity, and accessibility of information systems used by the private sector and other critical infrastructure. DHS supports Centers of Academic Excellence around the country to cultivate a growing number of professionals with expertise in various disciplines, including cybersecurity.

DHS S&T is leading efforts to develop and deploy more secure Internet protocols that protect consumers and industry Internet users. We continue to support leap-ahead research and development, targeting revolutionary techniques and capabilities that can be deployed over the next decade with the potential to redefine the state of cybersecurity in response to the Comprehensive National Cybersecurity Initiative. For example, DHS was a leader in the development of protocols at the Internet Engineering Task Force called Domain Name System Security (DNS SEC) Extensions. DNS SEC is necessary to protect Internet users from being covertly redirected to malicious websites and helps prevent theft, fraud, and abuse online by blocking bogus page elements and flagging pages whose Domain Name System (DNS) identity has been hijacked. S&T is also driving improvements through a Transition to Practice Program as well as liability and risk management protections provided by the Support Anti-terrorism by Fostering Effective Technology (SAFETY) Act that promote cyber security technologies and encourage their transition into successful use.

Growing and Strengthening our Cyber Workforce

We know it only takes a single infected computer to potentially infect thousands and perhaps millions of others. But at the end of the day, cybersecurity is ultimately about people. The most impressive and sophisticated technology is worthless if it's not operated and maintained by informed and conscientious users.

To help us achieve our mission, we have created a number of competitive scholarship, fellowship, and internship programs to attract top talent. We are growing our world-class cybersecurity workforce by creating and implementing standards of performance, building and leveraging a cybersecurity talent pipeline with secondary and post-secondary institutions nationwide, and institutionalizing an effective, ongoing capability for strategic management of the Department's cybersecurity workforce. Congress can support this effort by pursuing legislation that provides DHS with the hiring and pay flexibilities we need to secure Federal civilian networks, protect critical infrastructure, respond to cyber threats, and combat cybercrime.

Recent Executive Actions

As discussed above, America's national security and economic prosperity are increasingly dependent upon the cybersecurity of critical infrastructure. With today's physical and cyber infrastructure growing more inextricably linked, critical infra-

structure and emergency response functions are inseparable from the information technology systems that support them. The government's role in this effort is to share information and encourage enhanced security and resilience, while identifying and addressing gaps not filled by the marketplace.

Last month, President Obama issued Executive Order 13636 on Improving Critical Infrastructure Cybersecurity as well as Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, which will strengthen the security and resilience of critical infrastructure through an updated and overarching national framework that acknowledges the increased role of cybersecurity in securing physical assets.

DHS Responsibilities

The President's actions mark an important milestone in the Department's ongoing efforts to coordinate the national response to significant cyber incidents while enhancing the efficiency and effectiveness of our work to strengthen the security and resilience of critical infrastructure. The Executive order supports more efficient sharing of cyber threat information with the private sector and directs NIST to develop a Cybersecurity Framework to identify and implement better security practices among critical infrastructure sectors. The Executive order directs DHS to establish a voluntary program to promote the adoption of the Cybersecurity Framework in conjunction with Sector-Specific Agencies and to work with industry to assist companies in implementing the framework.

The Executive order also expands the voluntary DHS Enhanced Cybersecurity Service program, which promotes cyber threat information sharing between government and the private sector. This engagement helps critical infrastructure entities protect themselves against cyber threats to the systems upon which so many Americans rely. This program is a good example of information sharing with confidentiality, privacy and civil liberties protections built into its structure. DHS will share with appropriately cleared private sector cybersecurity providers the same threat indicators that we rely on to protect the *.gov* domain. Those providers will then be free to contract with critical infrastructure entities and provide cybersecurity services comparable to those provided to the U.S. Government.

Through the Executive order, the President also directed agencies to incorporate privacy, confidentiality, and civil liberties protections. It specifically instructs DHS to issue a public report on activities related to implementation, which would therefore enhance the existing privacy policy, compliance, and oversight programs of DHS and the other agencies.

In addition, the Presidential Policy Directive directs the Executive Branch to strengthen our capability to understand and efficiently share information about how well critical infrastructure systems are functioning and the consequences of potential failures. It also calls for a comprehensive research and development plan for critical infrastructure to guide the government's effort to enhance market-based innovation.

Because the vast majority of U.S. critical infrastructure is owned and operated by private companies, reducing the risk to these vital systems requires a strong partnership between government and industry. There is also a role for state, local, tribal and territorial governments who own a significant portion of the Nation's critical infrastructure. In developing these documents, the Administration sought input from stakeholders of all viewpoints in industry, government, and the advocacy community.

Their input has been vital in crafting an order that incorporates the best ideas and lessons learned from public and private sector efforts while ensuring that our information sharing incorporates rigorous protections for individual privacy, confidentiality, and civil liberties. Indeed, as we perform all of our cyber-related work, we are mindful of the need to protect privacy, confidentiality, and civil liberties. The Department has implemented strong privacy and civil rights and civil liberties standards into all its cybersecurity programs and initiatives from the outset. To accomplish the integrated implementation of these two directives, DHS has established an Interagency Task Force made up of representatives from across all levels of government.

Continuing Need for Legislation

It is important to note that the Executive order directs Federal agencies to work within current authorities and increase voluntary cooperation with the private sector to provide better protection for computer systems critical to our national and economic security. It does not grant new regulatory authority or establish additional incentives for participation in a voluntary program. We continue to believe that a suite of legislation is necessary to implement the full range of steps needed to build

a strong public-private partnership, and we will continue to work with Congress to achieve this.

The Administration's legislative priorities for the 113th Congress build upon the President's 2011 Cybersecurity Legislative Proposal and take into account two years of public and congressional discourse about how best to improve the Nation's cybersecurity. Congress should enact legislation to incorporate privacy, confidentiality, and civil liberties safeguards into all aspects of cybersecurity; strengthen our critical infrastructure's cybersecurity by further increasing information sharing and promoting the establishment and adoption of standards for critical infrastructure; give law enforcement additional tools to fight crime in the digital age; and create a National Data Breach Reporting requirement.

Conclusion

The American people expect us to secure the country from the growing danger of cyber threats and ensure the Nation's critical infrastructure is protected. The threats to our cybersecurity are real, they are serious, and they are urgent.

I look forward to working with this Committee and the Congress to ensure we continue to take every step necessary to protect cyberspace, in partnership with government at all levels, the private sector, and the American people, and continue to build greater resiliency into critical cyber networks and systems.

I appreciate this Committee's guidance and support as together we work to keep our Nation safe. Thank you, again, for the attention you are giving to this urgent matter.

Chairman ROCKEFELLER. Thank you, Secretary.

Now The Honorable Patrick Gallagher, who's Under Secretary of Commerce for Standards and Technology, and Director of the National Institute of Standards and Technology, which is in the U.S. Department of Commerce, and which is just chock full of Nobel laureates. It's one of the ultimate gems in Washington, D.C., and is not used as it should be.

Please proceed, sir.

STATEMENT OF HON. PATRICK D. GALLAGHER, PH.D., UNDER SECRETARY OF COMMERCE FOR STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE

Dr. GALLAGHER. Thank you very much. And it's a real pleasure to be here.

Let me begin by thanking both Chairmen Rockefeller and Carper, and both Ranking Members Thune and Coburn, and members of both committees, for the opportunity to testify today. It's a particular pleasure to be joining one of my critical partners in this effort, Secretary Napolitano.

Let me very briefly summarize NIST's role in our responsibilities to develop a framework for reducing cyber risk and critical infrastructure under the Executive order.

It may be a surprise to some that an agency of the U.S. Department of Commerce has been given this key role in cybersecurity but, in fact, NIST has a long history in this area. We have provided technical support to cybersecurity for over 50 years, working closely with our Federal partners. And also because NIST is a technical, but nonregulatory agency, we provide a unique interface with industry to support their efforts in technical and standards development. Today, NIST has programs in a wide variety of cybersecurity areas, including cryptography, network security, security automation, hardware roots of trust, and identity management.

As directed in the Executive order, NIST will work with industry to develop a cybersecurity framework that supports performance goals established by the Department of Homeland Security. DHS,

then, in coordination with sector specific agencies, will support the adoption of the cybersecurity framework by owners and operators of critical infrastructure and other interested entities through a voluntary program.

To be successful, two major elements have to be part of this approach:

First, it will require an effective partnership with DHS. Last month, I signed a Memorandum of Agreement with DHS Under Secretary Rand Beers to ensure that our work was fully coordinated with DHS.

Second, the cybersecurity framework must be developed through a process that is industry-led and open and transparent to all stakeholders. By having industry develop their own practices that are responsive to the performance goals, the process will ensure that it is both robust, technically, but also aligned with their business needs.

This approach has many advantages. It does not dictate specific solutions to industry, but promotes industry offering their own solutions. It allows solutions to be developed that are compatible with business and market conditions. And, by leveraging industry's own considerable capacity, it brings more talent and expertise to the table to tackle this topic.

This is not a new or novel approach for NIST. We have utilized very similar approaches in the recent past to address other pressing national priorities, notable examples being smart grid and cloud computing. We know how to do this.

Since this is industry's framework, the NIST role is to act as a convener and technical contributor. By working closely with our Federal partners, we also ensure that industry's work is relevant to their missions to protect the public.

So, what is in this framework? The short answer is, whatever is needed to achieve the needed cybersecurity performance, but, in practice, we expect the framework will include standards, methodologies, procedures, and processes that align the business, policy, and technological approaches to address the cyber risk for critical infrastructure.

Let me touch, briefly, on the topic of standards and their importance to success in this effort.

First, by "standards," I'm using the term as industry does. These are agreed-upon specifications, or norms, that allow compatibility of efforts to achieve a goal. These are not the same thing as regulation. Industry standards are developed through a multi-stakeholder voluntary consensus process, and it is this process that gives these standards their power and their broad acceptance around the world. These standards are not static. They can be changed to meet technological advances and meet new performance requirements. And, in fact, performance-based standards promote innovation specifically because they allow new products—services to be developed in a way that's not a tradeoff.

Mr. Chairman, I appreciate the challenge before us. This EO requires the framework to be developed within a year. A preliminary framework, in fact, is due within 8 months. We have already issued a request for information to gather relevant input from industry and other stakeholders. We are actively inviting those stakeholders

to participate in the framework process. The early response has been very positive.

Over the next few months, we will convene a series of workshops, where we will develop the framework, because this forum allows the necessary collaboration and engagement with industry. Our first organizational workshop will be held on April 3. In May, we will release our initial findings from the request for information, and our analysis of this response. And, by the 8-month point, we will have an initial draft framework, including an initial list of standards, guidance, and practices.

The President's Executive order lays out an urgent and ambitious agenda, but it is designed around an active collaboration between the public and private sectors. And I believe that this partnership provides the needed capacity to meet this agenda and it will effectively give us the tools to manage the cybersecurity risk we face.

And I appreciate the Committees holding this joint hearing. It's reflective of the partnership we'll need to be successful in this effort. And I look forward to answering any questions you may have.

[The prepared statement of Dr. Gallagher follows:]

PREPARED STATEMENT OF HON. PATRICK D. GALLAGHER, PH.D., UNDER SECRETARY OF COMMERCE FOR STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE

Introduction

Chairmen Rockefeller and Carper, Ranking Members Thune and Coburn, members of the Committees, I am Patrick Gallagher, Under Secretary of Commerce for Standards and Technology and Director of the National Institute of Standards and Technology (NIST), a non-regulatory bureau within the U.S. Department of Commerce. Thank you for this opportunity to testify today on NIST's role under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" and our responsibility to develop a framework for reducing cyber risks to critical infrastructure.

The Role of NIST in Cybersecurity

Let me begin with a few words on NIST itself: NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. Our work in addressing technical challenges related to national priorities has ranged from projects related to the Smart Grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips.

In the area of cybersecurity, we have worked with Federal agencies, industry, and academia since 1972 on the development of the Data Encryption Standard. Our role to research, develop and deploy information security standards and technology to protect information systems against threats to the confidentiality, integrity and availability of information and services, was strengthened through the Computer Security Act of 1987 and reaffirmed through the Federal Information Security Management Act of 2002. Consistent with this mission, NIST is actively engaged with industry, academia, and other parts of the Federal Government including the intelligence community, and elements of the law enforcement and national security communities, coordinating and prioritizing cybersecurity research, standards development, standards conformance demonstration and cybersecurity education and outreach.

Our broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users, from small and medium enterprises to large private and public organizations including agencies of the Federal Government and companies involved with critical infrastructure.

Executive Order 13636, "Improving Critical Infrastructure Cybersecurity"

On February 13, 2013, the President signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which gave NIST the responsibility to develop a framework to reduce cyber risks to critical infrastructure (the Cybersecurity Framework). As directed in the Executive order, NIST, working with industry, will develop the Cybersecurity Framework and the Department of Homeland Security

(DHS) will establish performance goals. DHS, in coordination with sector-specific agencies, will then support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities, through a voluntary program.

Our partnership with DHS will drive much of our effort. Last month I signed a Memorandum of Agreement with DHS Under Secretary Rand Beers to ensure that our work with industry for the Cybersecurity Framework, and also with cybersecurity standards, best practices, and metrics, is fully integrated with the information sharing, threat analysis, response, and operational work of DHS. This will enable a more holistic approach to addressing the complex nature of the challenge at hand.

A Cybersecurity Framework is an important element in addressing the challenges of improving the cybersecurity of our critical infrastructure. A NIST-coordinated and industry-led Framework will draw on standards and best practices that industry is already involved in developing and adopting. NIST coordination will ensure that the process is open and transparent to all stakeholders, and will ensure a robust technical underpinning to the framework. This approach will significantly bolster the relevance of the resulting Framework to industry, making it more appealing for industry to adopt.

Why This Approach?

This multi-stakeholder approach leverages the respective strengths of the public and private sectors, and helps develop solutions in which both sides will be invested. The approach does not dictate solutions to industry, but rather facilitates industry coming together to offer and develop solutions that the private sector is best positioned to embrace.

I would also like to note that this is not a new or novel approach for NIST. We have utilized very similar approaches in the recent past to address other pressing national priorities. The lessons learned from those experiences are informing how we are planning for and structuring our current effort. In 2009, the Energy Independence and Security Act (EISA) mandated NIST to develop a standards framework to help with the deployment of a nationwide, end-to-end interoperable Smart Grid. Following a similar approach to the one envisioned for the Cybersecurity Framework, NIST coordinated a forward leaning approach involving more than 1500 representatives from approximately 21 distinct domains that now constitute the Smart Grid.

This effort led to the development of a framework called the Smart Grid Roadmap that defined the domains of the Smart Grid and the interfaces for those domains, identified existing standards for these domains, prioritized standards needs and identified standards gaps. Many of these standards gaps are currently being addressed in various standards development organizations around the world. We are seeing the results of this effort pay off in many ways. Cybersecurity standards are being developed and adopted to secure different elements of the electrical grid. Standards based deployments of secure Smart Meters are enabling consumers safe and secure access to data about electricity usage. The U.S. Smart Grid Roadmap is being used as a template for frameworks in many countries around the world. Automakers are reaching agreement regarding chargers for electric vehicles. All these developments have helped address important policy objectives while also positioning the U.S. as a leader in Smart Grid development and deployment.

Another example of how NIST has brought together the public and private sector to address technical challenges is NIST's work in the area of Cloud Computing technologies. The unique partnership formed by NIST has enabled us to develop important definitions and architectures, and is now enabling broad Federal Government deployment of secure Cloud Computing technologies.

What is the Cybersecurity Framework?

The Cybersecurity Framework will consist of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks for critical infrastructure. Once the Framework is established, the Department of Homeland Security (DHS), in coordination with sector-specific agencies, will then support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities through a voluntary program. Regulatory agencies will also review the Cybersecurity Framework to determine if current cybersecurity requirements are sufficient, and propose new actions if it is determined they are insufficient.

This approach reflects both the need for enhancing the security of our critical infrastructure and the reality that the bulk of critical infrastructure is owned and operated by the private sector. Any efforts to better protect critical infrastructure need to be supported and implemented by the owners and operators of this infrastruc-

ture. It also reflects the reality that many in the private sector are already doing the right things to protect their systems and should not be diverted from those efforts through new requirements.

The Important Role of Standards in the Cybersecurity Framework

I'd like to explain why this approach relies on standards, methodologies, procedures and processes, and why we believe it to be a critical part of our work under the Executive order. First of all, by standards, I am referring to agreed-upon best practices against which we can benchmark performance. Thus, these are NOT regulations. Typically these standards are the result of industry coming together to develop solutions for market needs and are developed in open discussions and agreed upon by consensus of the participants. This process also gives standards the power of broad acceptance around the world. Standards have a unique and key attribute of scalability. By this I mean, that when we can use solutions that are already adopted by industry, or can readily be adopted and used by industry, then those same solutions reduce transactions costs for our businesses and provide economies of scale when deployed in other markets, which makes our industries more competitive.

A partnership with industry to develop, maintain, and implement voluntary consensus standards related to cybersecurity best ensures the interoperability, security and resiliency of this global infrastructure and makes us all more secure. It also allows this infrastructure to evolve in a way that embraces both security and innovation—allowing a market to flourish to create new types of secure products for the benefit of all Americans.

Developing the Cybersecurity Framework

NIST's initial steps towards implementing the Executive order include issuing a Request for Information (RFI) to gather relevant input from industry and other stakeholders, and asking stakeholders to participate in the Cybersecurity Framework process. This RFI was published last week and we are already getting informal feedback from industry and other stakeholders on the RFI. Given the diversity of sectors in critical infrastructure, these initial efforts will help identify existing cross-sector security standards and guidelines that are immediately applicable or likely to be applicable to critical infrastructure. Industry has begun responding to the RFI and is coming to the table to work with us on this analysis.

Underlying all of this work, NIST sees its role in developing the Cybersecurity Framework as partnering with industry and other stakeholders to help them develop the Framework. In addition to this critical convening role, our work will be to compile and provide guidance on principles that are applicable across the sectors for the full-range of quickly evolving threats, based on inputs from DHS and other agencies. NIST's unique technical expertise in various aspects of cybersecurity related research, technology development and an established track record of working with a broad cross-section of industry and government agencies in the development of standards and best practices positions us very well to address this significant national challenge in a timely and effective manner.

The approach of the Executive order will allow industry to protect our Nation from the growing cybersecurity threat while enhancing America's ability to innovate and compete in a global market. It also helps grow the market for secure, interoperable, innovative products to be used by consumers anywhere.

Next Steps

The Executive order requirement for the Framework to be developed within one year, and a preliminary framework due within eight months gives this task a sense of urgency. We have already initiated an aggressive outreach program to raise awareness of this issue and begin engaging industry and stakeholders. Over the next few months, NIST will bring many diverse stakeholders to the table through a series of "deep-dive" engagements. Throughout the year, you can expect NIST to use its capabilities to gather the input needed to develop the Framework.

In addition to the Request for Information (RFI), we are planning a series of workshops and events to ensure that we can cover the breadth of considerations that will be needed to make this national priority a success. Our first workshop will be held in early April to initiate the process of identifying existing resources and gaps, and to prioritize the issues to be addressed as part of the framework. In May, we are planning to release initial findings from early analyses of the responses to the RFI. This will mark a transition into the dialogue regarding the foundations of the framework.

In June, the Departments of Commerce, Homeland Security, and Treasury will submit reports regarding incentives designed to increase participation with the voluntary program. NIST will be supporting the report drafted by the Department of

Commerce, which will analyze the benefits and relative effectiveness of such incentives.

Around the five-month mark, in July, NIST will host a workshop to present initial considerations for the Framework, based on the analysis conducted with the responses to the RFI. This workshop will be the most in-depth of the three, with an emphasis on particular issues that have been identified from the initial work—including the specific needs of different sectors. At eight months, we will have an initial draft Framework that clearly outlines areas of focus and initial lists of standards, guidelines and best practices that fall into those areas

In a year's time, once we have developed an initial Framework, there will still be much to do. For example, our partners at the Department of Homeland Security will be working with specific sectors to build strong voluntary programs for specific critical infrastructure areas. Their work will then inform the needs of critical infrastructure and the next versions of the Framework. The goal at the end of this process will be for industry to take and update the Cybersecurity Framework themselves—allowing it to evolve when needed.

Conclusion

The cybersecurity challenge facing critical infrastructure is greater than it ever has been. The President's Executive order reflects this reality, and lays out an ambitious agenda founded on active collaboration between the public and private sectors. NIST is mindful of the weighty responsibilities with which we have been charged by President Obama, and we are committed to listening to, and working actively with, critical infrastructure owners and operators to develop a Cybersecurity Framework.

Thank you, for the opportunity to present NIST's views regarding critical infrastructure cybersecurity security challenges. I appreciate the Committees holding this joint hearing– it is reflective of the working partnership we have with Department of Homeland Security and other agencies to tackle cybersecurity issues. We have a lot of work ahead of us—and I look forward to working with both Committees to help us address these pressing challenges. I will be pleased to answer any questions you may have.

PATRICK D. GALLAGHER

Dr. Patrick Gallagher was confirmed as the 14th Director of the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) on Nov. 5, 2009. He also serves as Under Secretary of Commerce for Standards and Technology, a new position created in the America COMPETES Reauthorization Act of 2010, signed by President Obama on Jan. 4, 2011.

Gallagher provides high-level oversight and direction for NIST. The agency promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. NIST's FY 2012 resources total $750.8 million from the Consolidated and Further Continuing Appropriations Act of 2012 (P.L. 112–55), with an estimated additional annual income of $62.7 million in service fees, and $128.9 million from other agencies. The agency employs about 2,900 scientists, engineers, technicians, support staff, and administrative personnel at two main locations in Gaithersburg, Md., and Boulder, Colo.

Gallagher had served as Deputy Director since 2008. Prior to that, he served for four years as Director of the NIST Center for Neutron Research (NCNR), a national user facility for neutron scattering on the NIST Gaithersburg campus. The NCNR provides a broad range of neutron diffraction and spectroscopy capability with thermal and cold neutron beams and is presently the Nation's most used facility of this type. Gallagher received his Ph.D. in Physics at the University of Pittsburgh in 1991. His research interests include neutron and X-ray instrumentation and studies of soft condensed matter systems such as liquids, polymers, and gels. In 2000, Gallagher was a NIST agency representative at the National Science and Technology Council (NSTC). He has been active in the area of U.S. policy for scientific user facilities and was chair of the Interagency Working Group on neutron and light source facilities under the Office of Science and Technology Policy. Currently, he serves as co-Chair of the Standards Subcommittee under the White House National Science and Technology Council.

Chairman ROCKEFELLER. Thank you, sir.

I'm going to ask a question, and the four who spoke will too, but we'll be very brief, because there are a lot of people here. We're

going to go according to the early bird rule. To start, I'm just going to ask one quick question to both of you.

There are some people who say, "Look, the House basically has information sharing in its bill." It doesn't have much about workforce, it doesn't have much about standards, it doesn't have much about a lot of things, which I think are critical to a good bill, but it's in their bill, so, in theory, in that most people would agree with that, if you wanted to get a piece of legislation, you could just hold yourself back to information sharing. I think that's wholly insufficient. I don't think that's a wise, useful, constructive approach to the kind of bill that we can't really come back to each and every year. We've got to do our full work this year.

So, I'm asking, starting with you, Secretary Napolitano, do you think that information sharing alone is sufficient?

Secretary NAPOLITANO. No. I think you've got it right, Mr. Chairman.

In terms of the House bill, even in the information-sharing area, I think there were some deficiencies in it. It had no privacy protections built around it, which is very important in the—particularly in the civilian realm. And it resided almost all of the cybersecurity information monitoring responsibilities within the NSA, which, of course, is part of the military. We're talking about a totally different environment here, the domestic environment, the partnership with core critical infrastructure.

But, beyond that, what we are looking for is legislation that can, if necessary, put in statute the clarity of the roles and responsibilities now contained in the EO, so that that is preserved, moving forward; a bill that looks at the basic standard-setting that we need for core critical infrastructure of the country; a bill that addresses FISMA as we move, and try to move, from a paperwork-dominated statute to one that requires and embodies continuous diagnostics, in realtime; and increased research and development, among other things.

So, as we kind of lay out the topics involved under the umbrella of cybersecurity, information sharing is very, very important. Realtime information sharing is critical, but it is not the only concern we have in this arena.

Chairman ROCKEFELLER. Thank you.

Secretary Gallagher.

Dr. GALLAGHER. So, I think—it's hard to add to that answer, but I think cybersecurity doesn't lend itself to simple solutions. And I think, in the particular example you gave, even with information sharing, where you're going to provide threat information to the private sector, they have to have the capacity to act on that information. And, to do that, it involves some of the standards and technology issues that we're talking about in the framework.

So, I think these things tend to be interdependent and go hand-in-hand.

Chairman ROCKEFELLER. Senator Carper.

Chairman CARPER. Thanks, Mr. Chairman.

I'd like to go back a bit in time with each of you, and go back to when the Senate—particularly Senators Lieberman, Collins, Rockefeller, myself, Feinstein—offered the earlier version of our legislation, our comprehensive legislation. And, in it, critics said,

"Well, you've got the standards—with respect to standards," that's best practices, if you will, for critical infrastructure—"basically, you've got it mandated, and somebody telling us what to do. That somebody might be DHS." They didn't appreciate that very much. And the idea was rejected. So, we changed it.

As you know, we changed it so that—we came back and said, "Well, why don't we say that, for critical infrastructure, the best practices would be, not mandated, but we'd ask the industries—the owners, the operators of the critical infrastructure—to tell us what—or to tell the Department of Homeland Security what the standards ought to be. There would be a dialogue between—that includes DHS, NSA, FBI, others—and they would somehow—in this discussion, this roundtable, they'd figure out what the best practices should be." Again, there was a push-back from the—part of the business community said, "No, no, that's going to end up with—we'll end up with mandated best practices, mandated standards in that."

And so, we come up with this Executive order. And the Executive order says, as I understand it, "Your dance partner, owners of critical infrastructure, is not going to be FBI, it's not going to be Homeland Security, it's going to be Assistant Secretary Gallagher and our friends at NIST. And they work with industry all the time on stuff that's related to this, like"—that's one of the things that you talked about.

It's—what you've laid out, here, this framework, suggests to me that each time—it's the third major proposal, here—each time, it's been changed; and each time, it's been changed to reflect, maybe the legitimate concerns, or maybe not so legitimate concerns, that were raised within parts of the business community.

But, I think we've moved a long ways, y'all have moved a long ways, and, I think, in smart ways.

As my wingman here, Dr. Coburn, has suggested, there are still some concerns about liability protection. My understanding is, on the information-sharing sides, there's not so much—it's not so much an issue anymore. I think there may be bipartisan agreement with respect to punitive damages, and maybe general damages. I think there are some questions about liability protection on the critical infrastructure side. Should it be punitive? Should it be more than punitive?

But, there has been a whole lot of movement, as I see it, from the administration and, I think, from a bipartisan group of us in the Senate, to meet the legitimate concerns that have been raised.

Here's my question. Two-part. One, as you've gone out and done good work in seeking input, Dr. Gallagher, from the business community, what are you hearing? Is there any acknowledgment that changes have been made? In a sense, the administration is kind of negotiating against itself, but I think we're negotiating after hearing what's being offered by those who have been critical of our earlier approaches.

Number one, what are you hearing in response to the changes, this latest iteration? Positive, or not?

And, second—this is, maybe, more for our Secretary—on the liability side—general and punitive on the information sharing. That's pretty—most people say that's pretty good, in terms of give

to the business community. And the question is, what do we have to do in liability, on the critical infrastructure side, to get their buy-in.

Two questions.

Chairman ROCKEFELLER. And before those are answered, the vote is premature, but it has started—the cloture motion on John Brennan—so, we're going to work a tag-team thing here. Whether we're Republicans or Democrats, it makes no difference. I'm going to go over. John, you can run faster than I can.

Chairman CARPER. Mr. Chairman?

Chairman ROCKEFELLER. Yes.

Chairman CARPER. Someone just handed me a note. It says it's going to be—the first vote is on the Brennan nomination, the 3:15. If it's agreed to—and I'm encouraged that it's going to be agreed to——

Chairman ROCKEFELLER. Well, we're 10 minutes into it. It's already started.

Chairman CARPER. Oh, OK. OK. Fair enough.

Chairman ROCKEFELLER. Because we're going to have two votes.

Chairman CARPER. Good. We're going to have two votes. Fair enough.

Chairman ROCKEFELLER. OK.

Chairman CARPER. All right.

Chairman ROCKEFELLER. Go ahead and answer.

Chairman CARPER [presiding]. Yes. Two questions, please. Thank you.

Dr. GALLAGHER. So, very quickly, let me give you the reaction that I've been hearing from business. I think, generally, it's been very positive. And I think the origin of that reaction has to do with the tension that you've observed as these negotiations on how standards and requirements play off each other.

I think one of the reasons the reaction is positive is that I—and Senator Rockefeller mentioned this in his opening remark—the tricky issue here is that there is a public accountability for performance in the forum of critical infrastructure. If it fails, it causes impact to the nation. But, these type of standards and requirements also have business impact; they touch how businesses perform, they touch their business practices, and they affect the markets. And I think, generally, there's a reticence to having the government somehow have an undue impact on their business condition.

So, this arrangement allows, really, kind of the ideal choreography, because the Department of Homeland Security lays out the performance expectation—what do we have to achieve, from a cybersecurity-performance view?—and then charges industry with coming up with the business and cybersecurity practices that meet that goal. And then we try to align our practices.

So, in this complicated mix, where you want this to take place, I think this is the best of all possible worlds.

NIST is kind of an ideal convener, because we're technical and we're not in charge of anything. So, we can be sort of neutral and be a partner with industry as they develop that.

Chairman CARPER. Good.

Secretary Napolitano, the second half of the question, please.

Secretary NAPOLITANO. With respect to liability protection, I think the administration is already on record as having supported the targeted liability protections that were in the bill last year, the bipartisan bill last year. But, the EO also requires us to look at other ways to incentivize businesses to raise their practice to meet the standards that are ultimately seen as optimal. And so, for example, a—exploring, as we are, whether there could be a procurement preference, for example, given; whether there could be some kind of a seal of approval that is given. Now, those are just two ideas that can also provide incentives, because—recognize that the market, in and of itself, has not provided sufficient incentive, yet, for all business to voluntarily raise their standards.

Chairman CARPER. All right. This vote's started—thank you for—both of you—for those responses—the vote started about 8 minutes—9 minutes ago, and——

Thuney, you want to take a shot?

Senator THUNE. All right, thank you, Mr. Chairman, I will, and we'll race over there together.

Let me just, if I might, Secretary Napolitano, direct this question to you. The Executive order directs the Secretary of Homeland Security—you—to provide performance goals for the cybersecurity framework. We've been told the performance goals are intended to establish the level of security that the framework should meet. Doesn't the ability to set the performance goals put DHS in the driver's seat for this process, no matter how collaborative the initial NIST process may be?

Secretary NAPOLITANO. Well, we already do this, in the physical security side, with critical infrastructure. We work with critical infrastructure in 18 separate sectors to work on commonly understood performance goals and standards. So, in a way, Senator, this is simply extending that into the cyber realm.

But, we intend, and are pursuing, a realm that is very collaborative in nature. Our goal is to set performance goals. And NIST, then, establishes the framework and the standards of how those goals are reached.

So, by way of example, a goal might be for a major—let's say, a utility—if its major server, or servers, is attacked and is nonfunctional—to have the capability to restore service within a certain period of time. What the definition of that certain period of time is, is something that we would be working with, with industry, what makes sense, how would they do it, what are their options, and so forth. But, that would then feed into the framework that NIST will be establishing.

Senator THUNE. And just to elaborate on that a little bit, how do you intend to ensure that the performance goals are reasonably attainable by your private sector partners?

Secretary NAPOLITANO. Well, again, the EO requires us to engage in a collaborative process, and to make sure that all voices are listened to. And we do this in other areas already. So, I would say, again, we will simply take some of the lessons learned from some other things that we have done in the physical infrastructure realm, and continue them into cybersecurity.

Senator THUNE. All right.

Dr. Gallagher, how will NIST ensure that the framework that you're directed to develop with industry and other agencies does not undermine, conflict with, or duplicate existing mandatory—or voluntary, for that matter—government- or industry-led standards for each infrastructure sector?

Dr. GALLAGHER. So, the way we'd like to approach that is by having the industry and the critical infrastructure community put the framework together themselves. I think we've—we've done this approach in smart grid, where—and in cloud computing—where those same stakeholders, who are operating under either mandatory or industry-led standards, are quite willing to put those on the table; and that's actually the starting point for this framework process. This is not NIST developing new or additional material; this is much closer—much better thought of as a harmonization of what industry is presently doing, itself. So, that's the way of taking care of that conflict.

Senator THUNE. You mention, in your testimony, that—and I'm going to quote, here—"Many in the private sector are already doing the right things to protect their systems, and should not be diverted from those efforts through new requirements."

How are you going to work with DHS to ensure the Federal Government is not diverting companies with new requirements?

Dr. GALLAGHER. So, I think the way that this works is—and, in fact, the request for information we just put out asks companies and stakeholders to share with us their current practices and standards that they use. And I think the way this framework is going to look, at the beginning, is, you're going to see areas of overlap or where there's, you know, maybe, existing and—from—existing practices from different sectors that tackled the same problem in different ways. And there's going to be areas where there are gaps.

And so, the roadmap is going to have a very interesting sort of—the framework is going to have a roadmap character to it, where, you know, we can use that to address those areas of overlap and see whether that's a problem, or not. And I think the way—industry needs to lead those discussions, not us. And, conversely, when we see areas where there are gaps, then there's going to be the ability to organize and set priorities to address those gaps.

So, I think the process is specifically designed to make sure we don't reinvent the wheel.

Senator THUNE. And one quick question before we go vote—what's the threshold for sufficient industry feedback and participation in the framework development process? How are you going to ensure that you receive enough industry input?

Dr. GALLAGHER. That's an interesting question. I don't—we haven't had the problem of insufficient industry involvement in the past, so we're anticipating the opposite problem, which is an enormous insurge of participation. And I think what happens at the working level, through most of these efforts, is, you pick up on industry's own consensus-standards processes. And so, the same sort of criteria for whether the right stakeholders are involved and participating applies there.

And I think the final analysis is going to determine—is going to look at the quality of their work product. If the right folks were

around the table, and the best ideas were brought out, and then we're going to have the most viable product, I guess the final test of all would be the market, you know, pickup. I mean, the real test of the framework is whether it's put into practice. And if insufficient involvement was there, that's not that buy-in, then we're not going to see that adoption.

Senator THUNE. Mr. Chairman, I think we have to go vote.

Chairman CARPER. Yes, we do.

Senator THUNE. Recess?

Chairman CARPER. We're going to do a short recess, probably 10 minutes. We'll be back in about 10 minutes. Thank you for your patience and letting us go do our nation's work. Thanks so much.

We're in recess for 10 minutes.

[Recess.]

STATEMENT OF HON. MARK WARNER,
U.S. SENATOR FROM VIRGINIA

Senator WARNER [presiding]. Well, this may be the first and only time I get to chair this combined hearing, for the next 20 or 30 years, so I rushed back. We do have a second vote, but it appears that the first vote may take some extended time. There are some folks at the White House. So, hopefully Senator Coburn will be back shortly, as well, and we'll be able to continue to move on.

I wanted to look—and I know one of the biggest challenges we've got on this whole question is, you know, how we set appropriate standards, how those standards are nimble enough as a—in a field that is constantly evolving. As somebody who made a living in the technology field, I'm somewhat familiar with that. And I think Senator Coburn raised, appropriately, the right question, how we can then use the information sharing so that firms are able to share in a way that has both—appropriate protections in place.

And one thing that I would just add—since I may have a little bit more time, as folks come back—is that I sense that there is a changing feeling in the business community, because, one, the increased amount of cyber activities, cyber attacks; two, the publicly released Mandiant report, which cited and specified the activities, particularly coming from China, and how pervasive they are, and how much intellectual property is stolen. So, while I, clearly, want to make sure that businesses get the appropriate protections, I think there's an evolving feeling, in the business community, that standards that had some enforcement behind them, other than voluntary, are important.

And what I wanted to have, perhaps—Mr. Gallagher, start first—and then Secretary Napolitano address, is this—the free-rider issue. When you have a voluntary set of standards, and you have those businesses, entities that meet these standards, then those that don't, in effect, have that plain economic free rider effect. And is it not the case that, particularly within sectoral industries—take utilities, for a moment—you may have—because the—all the utilities have an enormous interconnection between them—those free riders who don't have appropriate protections in place may end up being an entry point, not only into their own operations, but then into other firms, because the firewalls between common industry partners are not as great.

So, if both of you would like a take a crack at this issue of the free riders—whether you see it, whether you're seeing an emerging feeling from the business community on this issue.

Dr. GALLAGHER. So, thank you, Senator Warner.

I think that, with regard to the accountability of the standards framework, you know, voluntary sometimes feels soft, as if it's optional. But, the term is used in business—in fact, standards developed through a voluntary consensus process by businesses can be, in fact, fairly muscular. They can include schemes that are there to identify whether products and services conform to those standards. And those conformity assessment vehicles, like product marking or various other things, can be used in their business-to-business relationships; they can be part of contract requirements, they can be part of their own procurement requirements, and so forth. And that's why these standards have such a powerful market effect, is that they start driving these interactions.

So, I don't think we should believe that, because business is in charge of the standards environment, that it's going to be weak. I think—as long as the accountability is there for the underlying cybersecurity performance, I think they're going to be inclined to look at making sure that there's a robustness there and they can identify their supply chain as not undermining their credibility.

That being said, there is going to be unevenness in adoption, and I think that's going to be one of the things we continue to monitor, both with the stakeholders who are helping us develop the framework and with our Federal partners. In some cases, it's going to be, maybe, willful; in other cases, it may be just the size of the company. Small businesses sometimes face different hurdles, in terms of compliance, than large companies. And hopefully that's a part of the framework and the partnership.

Senator WARNER. Before Secretary Napolitano answers, I guess the one thing I would just come back to you at little bit is, you know, the analogy, a little bit, breaks down where industry sets a standard, and there may be a marketing advantage. If you get the *Good Housekeeping* seal of approval, that helps you. A competitive product that doesn't have that *Good Housekeeping* seal of approval doesn't cause you any risk; whereas, within an industry—again, critical infrastructure, in particular—the weakest link could not only provide a way into your company, even though you've got the *Good Housekeeping* seal of approval, and cause harm, or, in addition, you know, you may have the weakest link, then cause such a problem that there could be industrywide repercussions even if you got—because you're not going to have any safe harbor provisions.

Secretary Napolitano, and then also you want to——

Secretary NAPOLITANO. Well, Senator, I think there is a risk, here. And the risk is the free rider risk, that all who need to be involved won't invest in order to be involved. But, I think it's a measured risk, compared to a process that is an open process, that involves industry from the get-go, and that really aligns well with what we've done on the physical security side, and with what NIST has done, in terms of other types of standard-setting.

One of the questions is, why wouldn't a company participate? One reason is that they, themselves, do not have the technical

know-how. They don't have the IT personnel, and the like, to really be able to participate.

One of the things we will be building and encouraging through this is the exchange of best practices. That exchange, among those actually in the market, actually can help smaller entities or those who have not invested what they should have, already.

And finally, as I mentioned in my opening, I think there's not just a *Good Housekeeping* seal-of-approval sort of incentive that we can build, but, again, looking at things like procurement preferences, acquisitions, and the like, that really, at least to the extent that government is a consumer of these services, can be helpful.

But, there is—as you have identified, this is, legitimately, a risk.

Senator WARNER. Well, I just personally believe that—I think this collaboration ought to be industry-led. I do believe there needs to be an enforcement mechanism, and I do think there needs to be, similar to some of the legislation that was introduced last year, standards that had some teeth to it. And, as Mr. Gallagher said, you can have standards with teeth that's industry-driven, but you've got to have some kind of enforcement tool.

I want to follow up, Secretary Napolitano, with your question of "those entities that might be in a particular sector that don't have the capabilities." You know, how do you make sure they are able to get the intellectual product that is being created by, you know, the large utility versus the small rural utility? If the large utility is spending lots of resources getting the best and the most efficient cybersecurity system in place, you know, they're going to be—they may be reluctant to share that benefit with partners who are, again, free riders. How do we get over that——

Secretary NAPOLITANO. I think——

Senator WARNER.—challenge?

Secretary NAPOLITANO. I think the way to think about that is their participation in the construct of the framework, because NIST really sits as kind of a neutral in the creation of the ultimate framework, but the framework itself provides a way for all entities involved in a particular area to exchange information. And I think we've seen that happen with some of NIST's other activities. So, the process itself could help solve that problem.

Senator WARNER. I'm not—I want Mr. Gallagher to—I'm not sure I fully got the answer, there, because I'm—you know, this is a very competitive space right now, as people come out with cybersecurity products and services. Some are better than others. You know, you've got—this will constantly be evolving. You know, one of the concerns, I know, is that we end up with a stagnant standard that kind of gets industry-accepted, technology moves ahead, and how do the new movers in that cybersecurity industry break in if you've already got a government-established standard? But, somehow or the other, we've got to figure this out.

Do you have any thoughts on it, Mr. Gallagher?

Dr. GALLAGHER. Well, I think—you know, I—that's one of the reason why we don't like to have government set standards in the United States. I think, by law, we have a preference, where Federal agencies look to the private sector standards organizations for their needs as the first preference. And one of the reasons for that

is, they tend to be more dynamic, because they're market-attuned, and they're going to keep looking at that.

The tension you point out, where it's a very competitive market—I mean, the standards process can be weaponized, as you know. Large companies can come in and want to, you know, take advantage of the—incorporating their technology in a standard because of the—the market advantage that would accrue to them if that was widely adopted. But, the standards processes have learned how to adopt to those kinds of commercial tensions in the process. That's really the kind of diplomatic negotiation that's occurring in the voluntary consensus standards process.

And so, we will be, not replacing that function, we'll—the framework process will be engaging existing standards development organizations and leveraging their expertise, and carrying that out.

Senator WARNER. Well—I've run over my time; I'm still not completely sure how we work that out on the free rider issue.

The last quick—very quick question, and I'll turn it back to Senator Coburn—it just—when we think about cyber threats, a lot of what's discussed in the press are those intellectual property threats and those threats that could actually interfere, turn on and off, operations. Do we—do you prioritize nature of threat, those that are simply, in effect, passive stealing versus those threats that are actually able to shut down critical infrastructure, for example?

Chairman CARPER [presiding]. I'm going to ask our witnesses just to be very brief in your response, please.

Secretary NAPOLITANO. In some senses, yes. I can explain later, when there's more time.

Chairman CARPER. That was good.

[Laughter.]

Chairman CARPER. All right, thanks.

Have you made the second vote? Yes, there is a second vote. Final passage. You know? OK.

Dr. Coburn.

Senator COBURN. Well, thank you.

Madam Secretary, I—one of the things—you have this great, big agency—in there—like on FISMA—do you really feel like you have the authorities you need, right now in your position, to actually accomplish what we need to do, especially when it comes to cybersecurity for the government?

Secretary NAPOLITANO. I think we can accomplish much with our existing authorities. As I've suggested, Senator, I think some FISMA reform, which would move us out of the paperwork generation into the Digital Age, very helpful, was considered part of the original legislation.

The ability to do hiring equivalent, with equivalency to the sorts of hiring that the NSA could do—because, realize, in this realm, civilian capacity needs to be enhanced, because we're going to manage most of this through civilian capacities, with some utilization of the NSA. And we already have those arrangements made. But, on that personnel side, we will need legislative assistance.

Senator COBURN. OK. Do you feel comfortable—and I'm not asking this question so you'll make a criticism of the Executive order—do you think we have the proper balance, in terms of intellectual property and protection of critical infrastructure, within the Execu-

tive order? We're going to help that, but what's your feeling about that?

Secretary NAPOLITANO. I think, overall, yes. And I think our key interests—and it's partially a response to Senator Warner, earlier—is the protection of the country from a cyber event that could cause undue economic loss or, in worst case circumstances, even endanger life. So, we fundamentally need to be concerned with that.

That kind of investment may not be as marketable or return-on-investment-oriented as, say, protection against the theft of your intellectual property. I mean, I think there's an easy economic case, "This is better for us, it's going to be better for our bottom line, it's part of the R&D process and our protection of our intellectual property."

In the security context, there's a public element to this that is not reflected immediately in the return on investment. That's why, from a standpoint of where we focus most of our efforts—we do the theft of intellectual property, the counterfeiting, the—all of that, those kinds of cases—but, where we are focused within the security of the United States is really on that fundamental attack, that fundamental interference that could shut us down.

Senator COBURN. Yes. You have all these areas of responsibility, and a large agency, and we're coming up on a tenth anniversary of your agency. And we had a great conversation, when I came out to visit you. But, there are—you have some real challenges. I mean, they're documented. GAO has documented, your own IG, as well as our investigative subcommittee. Do you—can you assure us you're seeing improvements in all those areas, and you're making the management adjustments those criticisms that have been rightly leveled, in terms of difficulties within the agency? Because your ability to respond to those has a lot to do with your ability to carry out the function that we're going to be giving you under the President's Executive order.

Secretary NAPOLITANO. Right. And I think—in terms of management of a Department that was brought together out of 22 agencies and is still relatively young, I think we have worked very closely with the GAO and the IG to really tighten the management and the accountability of the management, departmentwide.

I can also share with you that there has been no part of the Department that has expanded so rapidly, in terms of capability and responsibility, than the part that deals with cyber. And that's because of the continuing threat that we face.

Now, with the EO, we will take on even more responsibilities. Many of these are continuations of things we've done. Some of them are actual expansions. But, we are fully prepared to do that.

Senator COBURN. I have to tell you, I have been thoroughly impressed with the employees and the people that have given us the briefings that we've had. There's no doubt to their competence, their dedication, and their service. And I would just tell you, you should take that back.

Before my time's up, which it almost is, I would ask that you leave some people here to hear the GAO testimony after you leave, if you would. I think some of that some of this is spot on; some of it may not be. But, I think having this—the GAO outline where

they see the problems, and you hearing—somebody in your agency actually hearing that, and reporting to you what that is—and the flavor, and the insight that they have, I think will be beneficial as you work to implement what you're charged to do.

Secretary NAPOLITANO. Happy to do that, Senator.

Senator COBURN. Thank you.

Chairman CARPER. And I second that request. If you could, that would be great.

All right, I've been waiting to make this introduction for a while, but—Senator from Massachusetts, Senator Mo Cowan.

Senator Cowan.

STATEMENT OF HON. WILLIAM COWAN,
U.S. SENATOR FROM MASSACHUSETTS

Senator COWAN. Thank you, Mr. Chairman. Madam Secretary, Mr. Gallagher.

My first question, Madam Secretary, is to you.

First of all, before I offer it, I'd preface it by saying thank you for your testimony today, and thank you for your partnership with us up in the Commonwealth of Massachusetts. You and your team have been very helpful to us, and through some difficult times. We really do appreciate that.

But, to the issue at hand—and forgive me if I cover a territory that may have been covered while I was away for the vote—but, I want to talk a little bit about the concept about cybersecurity as it relates to, sort of, the concept of the weakest link in the chain. And we're going to hear testimony today from a CIO from a major company about—and this is my description, not his—the—sort of the platinum level of security, or focus on cybersecurity that they employ. And that's a very strong link in the chain.

But, while that may be true of Dow Chemical and other companies, is it fair to say that the failure of any market participant, particularly when it comes to critical infrastructure, to improve their defenses, on the cybersecurity side, to a minimum baseline standard leaves us all exposed, notwithstanding those platinum structures in place, and leaves us exposed, not only to some significant costs, but some significant security concerns?

Secretary NAPOLITANO. Senator, I think the—our efforts are to have everyone raised to a certain baseline standard. There may be entities that do more than that, but a certain baseline. And that should be attached with greater real time information sharing, because information sharing is a big part of this, and exchange of best practices, new technologies, and the like. But, there is no—there is no mandate, per se, in the Executive order. So, we are getting at this through a cooperative, voluntary regime.

Senator COWAN. And through that cooperative, voluntary regime—I just want to be clear—you do believe that there is—there is value in that minimum baseline standard across all players in this critical sector. Fair to say?

Secretary NAPOLITANO. Yes. I think it—there is value, because what we are trying to do is, in a realm where there is an increasing number and sophistication of cyber threats from a variety of actors, making sure we are best prepared, as a country, to prevent or, if necessary, respond, and to mitigate any damage.

Senator COWAN. And perhaps—this question, to you, Dr. Gallagher—I've talked to a number of folks with particular knowledge and expertise in this field, including Cynthia LaRose, of Mintz Levin, about privacy in cybersecurity issues, and the point has been made to me that the market participants, obviously, should play an important role with the government in establishing baseline standards that are out there, and there should be—the ability of the market player is to have a significant influence over what those standards are. But, if businesses may be left to their own devices, we may never get to a point where we can ensure ourselves that we've properly, across all critical infrastructure issues, sort of addressed cybersecurity, because of the difference in scale of entities and a difference in focus. Would you agree with that assessment?

Dr. GALLAGHER. I think, if it's not done correctly, that could happen. I think the challenge is—turning to private sector-led standard-setting when the public sector needs those standards means that there's an accountability of the private sector to that performance. In other words, the—it's not the same thing as saying there's an abrogation of responsibility by the public sector by saying we want industry's help in doing it.

So, I think the EO correctly lays this out. It starts with a process where we try to articulate the cybersecurity standard of performance that we'd like to engage on. And then we let industry, who knows the market, who understands their technology, who understands the dynamics, attempt to respond to that.

In the final analysis, I guess the public sector will have to evaluate whether that meets the public's needs to secure the safety of the U.S. population, and respond accordingly. But, we do this very often. I think, you know, it's not uncommon for government agencies, in procurement and regulation and so forth, to depend on the private sector. And, in fact, the private sector wants to be responsive to that, generally, because they want their efforts to be aligned with those needs.

Senator COWAN. Thank you.

Chairman ROCKEFELLER [presiding]. Senator Johnson.

STATEMENT OF HON. RON JOHNSON, U.S. SENATOR FROM WISCONSIN

Senator JOHNSON. Thank you, Mr. Chairman.

Madam Secretary, Mr. Gallagher, thanks for coming before us.

Mr. Gallagher, I was actually pleased to see, in your testimony, that you said the approach should not dictate solutions, but, rather, facilitate it. I think that was one of the things that kind of bogged us down last time, when we tried to pass a cybersecurity bill.

And this is really a question for both of you. As you have gone around and talked to industry—certainly my input was, I think, last time around, there was an assumption, or a presumption, that business had to be dictated to. You know, I come from industry. I really think businesses want to protect their cyber assets and realize that government really has a real role to play here, and has a lot of valuable information.

So, can you just give me your evaluation, in terms of that—I guess, that assessment? How willing is business? How often do they really have to be nudged along a little bit more forcefully?

Madam Secretary.

Secretary NAPOLITANO. In general, the responsible business players recognize the multiple interests involved, and our work is furthered when there's truly a collaborative atmosphere. We all want to solve problems. No one is benefited if there's a major or successful cyber attack within the United States. So, we're approaching it from that dimension.

To the extent this is a national security issue, which it is, and we are leaving it to a collaborative process to help resolve, that is a first. Normally, when security is concerned, it is much more of a government, kind of, top-down, as it were, philosophy. So, this is a grand and bold experiment, in that regard. But, I proceed on the notion that we can make this work, and that we will.

Senator JOHNSON. Thank you.

Mr. Gallagher.

Dr. GALLAGHER. I would confirm that. I don't want to talk about the irresponsible players, but, I mean, my reaction, in working with business leaders, particularly in critical infrastructure, is, they acutely feel their obligation to protect the public, and want to perform.

I think the underlying issue—and this touches on some comments that Senator Warner raised, as well—is, this will work best of all when good cybersecurity is also good business. And when that alignment occurs, I think that's when the magic happens and this really works very powerfully. And that's related to this discussion on incentives. And I think one of the things that can come out of this process, since this is an industry-led standards development effort, is, we will be monitoring those areas where the standard-setting and adoption seem to be—where there seems to be a headwind that is related to, maybe, disincentives or, you know—and those will be important information for us to pay attention to. But, I think that's where this wins most dramatically, is when good security is also good business.

Senator JOHNSON. Now, last time around, the regulations were stated to be voluntary, but I think businesses viewed that as saying, "Yes, it was voluntary, but pretty coercive, particularly after 1 year." What has changed? Because it sounds like the reaction from businesses has changed pretty dramatically. I mean, what, specifically, did you change, in terms of that voluntary nature of the EO, in your proposals?

Secretary NAPOLITANO. I think one of the things that happened is that there was a process, led by the White House, to engage business in the construction of the EO, itself. So, it didn't just kind of spring like, you know, Athena from the head of Zeus, but it was really a collaborative process to begin with.

So, it's, you know—and the second thing I would mention, Senator, is, we have—we didn't stop work because the bill failed. I mean, we were already, all summer, you know, working on, How do we make sure that we are looking at adequate cyber performance goals? And what could standard-setting look like in this regime? So—and I think that gave, perhaps, assurance to some in the

business community that we truly are engaged in a collaborative process.

Senator JOHNSON. OK. One of my assumptions is that just the word "comprehensive" makes things more difficult around here. There are certainly different components to cybersecurity that could potentially—I'm just saying potentially—could be enacted in a step-by-step basis.

First of all, do you agree with that? Does it have to be comprehensive? And if it could be a step-by-step approach, do you have a priority? I know, Mr. Gallagher, I think you've listed the five pieces of legislative actions that are required. But, is comprehensive required, or, if it's not possible to get that, can we go step-by-step?

Dr. GALLAGHER. So, I think the problem with cybersecurity, of course, is, you're talking about a system behavior. And so, in the end, you have this problem, where it's a chain of performance, and you're as strong as your weakest link. And that's one of the reasons that you always have to think about the whole.

But, you're right, in order to make progress, you can't boil the whole ocean at once, and I think you have to set priorities. I think the Executive order, and this process, will allow that to happen. Clearly, part of this is dealing with known threats and known vulnerabilities, just good cyber hygiene and putting it into practice robustly. Some of this is putting in the tools that allow us to do adaptive cybersecurity. How do we react to the new information, the new threat information, the type of cybersecurity automation tools? And some of this is, how do sector-specific organizations address, you know, their requirements in the—you know, in their context, to protect the public, in the advent of a cyber.

So, it's a complicated challenge, in the sense that the whole matters, but you have to work at it in pieces.

Senator JOHNSON. OK, thank you.

Chairman ROCKEFELLER. Senator Baldwin.

STATEMENT OF HON. TAMMY BALDWIN,
U.S. SENATOR FROM WISCONSIN

Senator BALDWIN. Thank you, Chairman Rockefeller and Ranking Member Thune. Thank you, to my Chairman, Carper, and Ranking Member Coburn.

I'm new to the Senate, new to the Homeland Security and Governmental Affairs Committee, but, back in my House service, I had the opportunity to serve on the House Energy and Commerce Committee, where I started to become more aware, and sometimes more alarmed, about our need to protect our critical infrastructure and the threats faced by cyber penetrations, et cetera. And I look forward to the opportunity to be involved in this issue, moving forward, but looking at it more broadly than just the jurisdiction of the Energy and Commerce Committee, although it was pretty broad.

In that vein, I wanted to start, Madam Secretary—in your testimony, you briefly referenced the National Cybersecurity and Communications Integration Center, which is a 24/7 response center for potential cyber threats. And I wonder if you could describe for me in greater detail the sort of—the functions of this center, what sort

of business it's seeing, and if you could highlight a few stories of success that have been achieved through the creation of the center.

Secretary NAPOLITANO. The NCCIC, as we refer to it, is a 24/7 watch center. It has a number of partners on the watch center. Importantly, both the NSA and the FBI are partners there, as we are partners with the FBI in the—their JTTF center, as we partner with the NSA, as well. So, when you think about roles and responsibilities, the DHS, the FBI, and the NSA have really figured out for themselves the lanes in the road and how a call to one is a call to all.

It is constantly getting information. It gets reports from the private sector. It sends information out. It deals with mitigation efforts. It deploys teams to help mitigate damage, particularly in the area of industrial control systems. It's a very important subset of this that we've seen a lot of activity in. It really is our key information collection, sharing, collating, analysis area in the cyber realm.

One recent area we've been heavily involved in is a whole spate of DDOS attacks against the financial sector, and assisting them in responding, and also helping them to work around the DDOS attacks that they are experiencing.

I would invite you or any members of the Committees. We'd be happy to host you at the NCCIC to see what really has been built out there.

Senator BALDWIN. Thank you. You mentioned, in your response, working with industries that have industrial control systems. And want to sort of ask a related question. I was talking about my experience, in the House, on Energy and Commerce, and the cybersecurity issues that are raised there. I understand, from what I've been learning lately, that the financial services industry has some of the best protections in place against cyber threats, and certain, you know, other sectors that are protecting essential infrastructure have more lax protections in place, how we say.

I guess I'm wondering how the best practices from the financial services industry can be applied to other sectors, and to what extent the absence of industrial control systems in that sector hinder the application of those best practices. What's—what can go across sectors and be learned, and the fact that they don't have SCADA systems, you know, that it's not going to be that helpful in the other sectors?

Secretary NAPOLITANO. One of the things about cyber is that this is not—although we talk about sectors, they're not stovepiped, they're all interconnected. We live in a interconnected world, in every respect. There are some things that are being done in the financial sector that will easily migrate into performance goals, and, indeed, perhaps even into a framework. There are other things that are not as——

Senator BALDWIN. Can you——

Secretary NAPOLITANO.—applicable.

Senator BALDWIN.—can you outline—or can you mention some of those, just so I get a clear sense of what can migrate easily?

Secretary NAPOLITANO. I'd rather not, in an open setting.

Senator BALDWIN. Oh, OK.

Secretary NAPOLITANO. But, we'd be happy to provide a briefing for you.

Senator BALDWIN. Great. And I cut you off. You were saying, there are some things that migrate easily.

Secretary NAPOLITANO. And some that don't. But, to the—you know, one of the things that we will be working on with NIST is, as we set performance goals, and as we engage in this process, what does the framework absorb by way of things that are interconnected and that apply across a broad spectrum.

Senator BALDWIN. Thank you.

Chairman ROCKEFELLER. All right.

We go now to Senator Pryor. And then, that'll be the end of the first panel.

And I want to apologize to the first panel, because we've kept you here a long time. Part of it was my fault, but I apologize.

Senator Pryor.

STATEMENT OF HON. MARK PRYOR,
U.S. SENATOR FROM ARKANSAS

Senator PRYOR. Thank you, Mr. Chairmen. And I use that word in the plural. Thank you all for your leadership on this.

Secretary Napolitano, always good to see you. Thank you for being here again today. You mentioned, just briefly, something in your opening statement about the sequester and some of the adjustments you're going to have to make this year. Could you elaborate on that?

Secretary NAPOLITANO. Well, as you know, the sequester applies virtually account—it does apply account-by-account across the government, and limits our flexibility, in terms of where we put resources. The result is, for example, in our CERT teams, we were looking at, I think, a 10 to 12 percent reduction there, in terms of being able to fill vacancies. We are, importantly, I think, probably going to have to delay the deployment of the next generation of security for the civilian aspect of the Federal Government, the so-called E3A program, for a year, because we just are not going to be able to meet the deadlines, given the lack of resources that had previously been budgeted. So, those are two concrete things I can give you.

Senator PRYOR. Thank you.

Dr. Gallagher, do you have similar impacts from the sequester?

Dr. GALLAGHER. Similar, but not nearly at that scale. So——

Senator PRYOR. We understand, sure.

Dr. GALLAGHER.—yes, I think, for NIST, the reductions—so, the main role of NIST in the Executive order is one of convening and technical support. So, obviously, those are the two areas. But, by intentionally pivoting this so that this is an industry-driven process, I am hopeful that there is a very minimal impact on our ability to deliver the framework with the sequester. I think the real impact of the budget, in this particular case, is going to be more a long-term one, as—because I see the framework process as being a continuous one, and I hope it doesn't impact our ability to provide technical support to that ongoing process.

Senator PRYOR. Yes, that actually was my next question for you, because I assume that, if we do cybersecurity—and I hope we do—that you will have an ongoing role, but, at some point, obviously, resources have to be a consideration for you. So, in a shrinking

budget environment, have you thought through how you're going to manage that, or do you have enough information yet?

Dr. GALLAGHER. Well, the way you manage that is by setting some priorities. And I—you know, our priorities, in supporting standards coordination, are to support the highest priorities of other agencies. So, the NIST role in supporting standards is one of direct support to other agencies. So, it's hard to see that cybersecurity's not going to be at the top of that list. So, it may impact other priority areas.

Senator PRYOR. Right. I understand. And that—I think that's a concern of both committees, here.

Dr. Gallagher, next month you're having a—sort of a public workshop in Gaithersburg, I believe. What are you hoping to accomplish with that? And is that going to be the only one, or will others follow?

Dr. GALLAGHER. It will be the one—one of several. We anticipate at least four workshops, over the next 8 months, to develop the framework. We learned, from both our cloud computing efforts and from the smart grid standards efforts, that these type of robust workshops were a very powerful way of bringing together the stakeholders, because you've got to put a mix of stakeholders in a room and hammer out some of these issues. You can get pretty far with calls for information, and people submitting things. But, in the end, there has to be direct negotiation.

So, the first meeting is organizational. It's going to be, How do we set up the framework process to be productive? Hopefully, we'll be looking at what the performance objectives from DHS start to look like and how do we organize the effort so that we can produce the initial framework in 8 months.

Senator PRYOR. And is this a workshop just for public sector, or is it public and private?

Dr. GALLAGHER. We're going to invite everyone who can contribute.

Senator PRYOR. OK. So, how many people is that going to be, or how many organizations——

Dr. GALLAGHER. I'm—well, in the case of smart grid, we were up over 1600 people fairly quickly, and this is a broader area, so it could be quite large.

Senator PRYOR. Do you include—are you including State and local governments——

Dr. GALLAGHER. Yes.

Senator PRYOR.—in that? Good.

Mr. Chairman, thank you. That's all I have. Thank you.

Chairman ROCKEFELLER. Thank you, Senator Pryor.

I think Chairman Carper wants to say something, as you go, but stay, for the moment.

Chairman CARPER. Real brief.

Thanks very much for coming. Thanks very much for your work and the work of a lot of folks that you lead, for getting us this far.

A reporter asked me, earlier today, if the Executive order might be seen as an excuse for us not legislating; maybe we don't need to do much heavy lifting on—in the—on the legislative side. And I said, "No, I think it's an incentive for finishing the work that we began in earnest in the last Congress." And I'm encouraged, today,

that we've moved even further, and that we're—I'm encouraged that we're going to get this done.

So, Mr. Chairman, and to our panel, thank you so much.

Chairman ROCKEFELLER. I share similar sentiments. I'm very grateful to you both. Testifying probably is not the thing you most enjoy in life, but you were very helpful. You're both very smart, you both run very important organizations. Thanks a lot.

Our second panel will be—now, I pray I get this right; Senator Thune has tried to help me—Mr. Greg Wilshusen—is that a thumbs-up or a thumbs-down?

Mr. WILSHUSEN. Thumbs up.

Chairman ROCKEFELLER. Thumbs up, okay—who's Director of Information Security Issues for the U.S. Government Accountability Office. He was invited by Senator Thune and all of us. And also, Mr. David Kepler, who is Chief Sustainability Officer and Chief Information Officer, Business Services and Executive Vice President at a small company called Dow.

We welcome you.

And why don't you go—are you friends now?

[Laughter.]

Chairman ROCKEFELLER. OK. Why don't you go first, Mr. Wilshusen. Yes.

STATEMENT OF DAVID E. KEPLER, CHIEF SUSTAINABILITY OFFICER, CHIEF INFORMATION OFFICER, BUSINESS SERVICES AND EXECUTIVE VICE PRESIDENT, THE DOW CHEMICAL COMPANY

Mr. KEPLER. Thank you, Chairman Rockefeller, and thank you, Chairman Carper, as well, and Ranking Member Thune and Ranking Member Coburn.

I'm the Chief Information Officer and Chief Sustainability Officer for The Dow Chemical Company, and Dow appreciates the opportunity to provide our view on the state of cybersecurity in the U.S. today.

Today's companies regularly have to manage major information security issues, including corporate espionage, intellectual property theft, hactivists, attacks on our systems, and cyber criminals. Companies also have to be prepared to manage and mitigate risks, such as acts of terrorisms or sabotage, that may have severe physical and/or financial consequences.

As an example, Dow monitors and logs approximately 300 million generic network events a day. This gets distilled down to about 300 investigations each day, and results in about 10 mitigations we have to address. We manage an incident a month. This requires a major team effort, with a multi-day event—a multi-day team response.

So, companies have a vested interest, along with a duty to their stockholders, employees, and communities, to protect and defend their facilities, processes, and intellectual property against these cyber inclusions. However, industry must rely on the Federal Government to approach cybersecurity to deploy an offensive perspective by preempting attacks, when possible, through the pursuit and prosecution of criminals behind these events.

Since 9/11, The Dow Chemical Company, and many other chemical companies, have made significant investments in the areas to improve security. For example, the American Chemistry Council, as part of its responsible care approach, devised the security code which requires companies to adhere to the chemical industry best practices for both cyber and physical security.

Dow believes that the protection of the country's infrastructure can be addressed most effectively by moving forward with policy which strengthens the collaboration between the Federal Government and the private sector. These key principles of collaboration are, one, advancing more specific and timely information sharing between government, industry, and among industry peers; two, reasonable protection for sharing threat or attack information between the government and other companies; and, finally, it also has to lead to aggressive pursuit and prosecution of criminal—cyber criminals.

Dow does not support prescriptive regulation legislation or specific technologies or methods. Legislations that set up a system requiring significant resources to comply with this type of regulatory framework and the resources from addressing the threats and risks we need for mitigation. Issues around cybersecurity are in constant flux, and proper management requires a fluid and fast risk-based response. Complex regulatory mandates will only slow the advancement of cyber risk and management systems.

Effective two-way cybersecurity and physical information sharing must be linked together, and it must be timely, specific, and actionable, to help promote the flow of information. Information provided by the private sector and government should be adequately protected.

On liability, the protection afforded under the Support Antiterrorism by Fostering Effective Technologies, or the SAFETY Act of 2002, we think are appropriate for consideration for cybersecurity.

I was asked to comment on the Executive order on improving cybersecurity, and Dow supports the information-sharing initiatives included in the order. I believe we need to do more, in the long run. If there is anyplace for new legislation, it is to provide reasonable protection for information sharing to incur a broader-based sharing in the industries with government.

Leveraging security standards into the government procurement practice is a good idea.

Section 7, describing the cyber framework, I think this reflects a good sentiment and an approach; however, we do need to recognize that sector specific approaches and a clear willingness to build on prior work that private sectors have done is important. And this can't be a one-size-fits-all model, based on the industries we're trying to manage in the critical infrastructure.

Section 9, the declaration of risk and managing the criteria for reasonable result in an incident, needs to be better defined. The concern is, we'd create a large list of risks that are not clearly prioritized within a sector, and then push generic standards into that sector that's trying to manage the systems that they have to deal with, both in physical and cybersecurity.

Also, there needs to be more clarity on the position, in Section 9, that the Secretary shall not indemnify any commercial information technology products or consumer information technology services under this section. I hope this doesn't mean that the IT industry gets a free pass. We need their help in making this a successful endeavor.

The concept of a partnership is to work together on a common goal. The outcome of the effort, in cybersecurity, should not be measured by how many regulations we create, but how much progress we make against a real threat to our country's security in progress. We are here to do our part.

Thank you.

[The prepared statement of Mr. Kepler follows:]

PREPARED STATEMENT OF DAVID E. KEPLER, CHIEF SUSTAINABILITY OFFICER, CHIEF INFORMATION OFFICER, BUSINESS SERVICES AND EXECUTIVE VICE PRESIDENT, THE DOW CHEMICAL COMPANY

The Dow Chemical Company appreciates the opportunity to submit these written comments to the Senate Committee on Commerce, Science, and Transportation and the Senate Committee on Homeland Security and Government Affairs. We applaud the Committee for holding a hearing on cyber security and the necessary collaboration between government and the private sector.

About Dow

Dow was founded in Michigan in 1897 and is one of the world's leading manufacturers of chemicals, plastics and advanced materials. Dow combines the power of science and technology to passionately innovate what is essential to human progress. Dow connects chemistry and innovation with the principles of sustainability to help address many of the world's most challenging problems such as the need for clean water, renewable energy generation and conservation, and increasing agricultural productivity. Dow's diversified industry-leading portfolio of specialty chemical, advanced materials, agrosciences and plastics businesses delivers a broad range of technology-based products and solutions to customers in approximately 160 countries and in high growth sectors such as electronics, water, energy, coatings and agriculture. More information about Dow can be found at *www.dow.com.*

Cyber Security: A Manufacturing Company's Perspective

Cyber threat activity across the business community and the government has continued to increase over the last decade. The main driver of this change is in the profile of the threat itself which has matured from random acts primarily by individuals to now include well resourced organizations outside the United States. These new threats are targeted in areas that range from commercial espionage to terrorism to activism. Companies have a vested interest—along with a duty to their stockholders, employees and communities—to protect and defend their facilities, processes and intellectual property against these cyber intrusions.

The Dow Chemical Company and many other chemical companies have made significant investments in all of these areas to address cyber threats. After 9/11 for example, the American Chemistry Council (ACC), as part of its Responsible Care® approach, devised the Responsible Care Security Code which requires companies to adhere to the chemical industry best practices for security, both physical and cyber. Dow has invested heavily in, and is constantly upgrading, the physical and information defensive protection systems guarding our Company. However, industry must rely on the Federal Government to approach cyber security, working in partnership with other countries, to deploy an offensive perspective by preempting attacks when possible and through the pursuit and prosecution of the criminals behind these threats.

The management systems rely on information and knowledge, and there is a need for identifying better approaches to work with government in improving information sharing. Increased focus on real time and efficient information sharing programs should be improved to foster, incentivize and increase the sharing of threat activity.

Dow believes that protection of the country's critical infrastructure can be addressed most effectively by moving forward with legislation which strengthens the collaboration between the Federal Government and the private sector. The key principles of this collaboration are:

- Timely information sharing between government and industry and among industry peers.
- Reasonable protection for companies sharing threat or attack information with the government and their industry peers.
- Aggressive pursuit and prosecution of cyber criminals.

IT and telecommunication suppliers must continue to improve the security of their products and services and be unified in providing services that their customers can rely on for threat response.

Dow does not support prescriptive regulatory legislation on specific technologies or methods. Legislation that sets up a system requiring significant resources to simply comply with a regulatory scheme diverts resources from addressing the threats and risks in need of mitigation. Issues surrounding cyber security are in constant flux and proper management requires a fluid and fast response. Complex regulatory schemes will only slow the advancement of cyber risk management systems.

Background

The Internet has become critical to the operations of business, government and global commerce. It is an open and dynamic venue for the exchange and collection of ideas and information. For the United States it has been a key enabler for maintaining the country's competitiveness. Some elements inside and outside the country, however, have seized on this open framework and have found innovative ways to use it for illegal financial gains, victimization of the innocent and to advance ambitions that are not in the interest of the United States. Today, companies regularly have to manage major information security issues, including: corporate espionage, intellectual property theft and malicious activism. Companies also must be prepared to manage and mitigate risks such as acts of terrorism or sabotage that could have severe physical and/or financial consequences. The Dow Chemical Company, like many large corporations, is regularly attack from sources that are advanced, persistent and targeting our intellectual property. In many cases, the highly sophisticated attackers are based in foreign countries.

Efforts to develop a public-private partnership to protect against cyber attacks has a long history. In 2003, one of the key objectives of the National Strategy to Secure Cyberspace was to provide a framework for public and private partnership including the sharing of information. Much progress has been made, but today's cyber attacks are much more advanced and it is clear that more ongoing progress is needed to ensure the continued prevention of a severe systemic failure of public or private critical infrastructure. It will require a more responsive, integrated, and resilient national system to prepare for and respond to these threats.

Chemical Industry Cyber Security Leadership

Large companies such as Dow are seeing an increase in the risks we face. The internet, including the growth of social media, has elevated our exposure to threat actors such as hacktivists (hackers with a targeted malicious intent to vandalize or stop business as their protest method) and nation states sponsoring industrial espionage or cyber criminals. As society and industry move toward increased mobility and pervasiveness of information technology, the frequency and cost of cyber-incidents will continue to increase. These risks require a joint public and private effort to be managed effectively.

In 2001, Dow and other American Chemistry Council (ACC) members voluntarily adopted the Responsible Care® Security Code (RCSC). The RCSC is a comprehensive security management program that addresses both physical and cyber security. It requires a comprehensive assessment of security vulnerabilities and risks to implement protective measures across a company's value chain. Since RCSC's inception, ACC members have invested more than $11 billion in security enhancements including both physical and cyber security protections. Security, in all its dimensions, continues to be a top priority for Dow and the chemical industry. Our record of accomplishment and cooperation with Congress, DHS and others is undisputed.

Dow has led in several business and public forums which focus on advancing cyber security within the chemical sector. Dow regularly provides leadership or participates with the following organizations:

- *ChemITC*
  - Chemical Information Technology Center (ChemITC®) of the American Chemistry Council (ACC) is a forum for companies in and associated with the ACC to address common IT issues. Through strategic programs and networking groups dedicated to addressing specific technology issues, ChemITC® is committed to advancing the cyber security of its member organizations.

- *Chemical Sector Coordinating Council (CSCC)*
  - Pursuant to the Homeland Security Act of 2002, the purpose of the CSCC is to facilitate effective coordination between Federal infrastructure protection programs, the infrastructure protection activities of the private sector and those of state, local, territorial and tribal governments.
- *National Infrastructure Advisory Council (NIAC)*
  - The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of critical infrastructures, both physical and cyber, supporting sectors of the economy.
- *International Society for Automation (ISA)*
  - ISA has primary responsibility for the development of the ISA–62443 series of standards addressing cyber security for industrial automation and control systems (IACS). As each standard is developed it is submitted *simultaneously* to ANSI and IEC as a U.S national and international standard, respectively.

Cyber Security Management at the Dow Chemical Company

Dow has a comprehensive set of policies, standards and procedures based on guidance from organizations such as the National Institute of Standards and Technology (NIST) and established industry standards such as ISO 27001 and the ISA/IEC 62443 series for industrial automation. Due to the very fluid nature of cyber threats, Dow is continuously refreshing its practices and technology based on its experience as well as the best available information from the government, industry and other public sources. We frequently benchmark with peer Chemical Sector and broader Manufacturing Sector companies as well as other industries to manage the risk of a cyber attack. We also enlist external private entities to evaluate our security posture.

Dow's information security is based on a multi-layer defense strategy. This includes continuing to enhance our IT infrastructure to meet the standards of other companies with high-value security profiles as well as elevating the protection for the Company's most sensitive intellectual and physical assets. Dow uses a risk-based approach for the implementation of these controls. Developing strong partnerships between Dow's Information Security group and all Dow business units is vital to managing the flow of sensitive information and protecting critical infrastructure.

Strong collaboration with security vendors and partnerships with government agencies have been essential in preventing, detecting and responding to threats. We work closely with the chemical sector liaisons from the Department of Homeland Security and in forums such as the Industrial Control Systems Joint Working Group (ICSJWG). Working with government agencies has been valuable due to their collaborative nature. Dow believes that a public-private sector collaborative approach to cyber security is the best way to achieve common security goals for individual companies as well as the country. Using a risk-based approach that leverages the existing work of the international cyber security community will facilitate implementation of practices that are both effective and flexible.

Dow's multi-layer defense strategy begins with employees. Our ongoing security awareness programs help employees understand the ever-changing threats in the cyber landscape. People are the new perimeter—our greatest defense, and if not informed and educated, could be our weakest link. We have an ongoing global awareness campaign to:

(1) Educate users on policies and the risks we face;

(2) Drive commitment to the security program by making security initiatives a personal responsibility;

We continue to evaluate and improve the technical and non-technical response capabilities related to cyber threat incidents and we have made significant investments in state-of-the-art technologies to detect anomalous cyber activity which is the predecessor to most cyber attacks. Dow has defined threat response processes to handle these issues when detected and has established a core team of highly skilled employees to coordinate response and proactively mitigate risk to the Company's systems. In order to maintain a highly secure environment, Dow has a team of security professionals who regularly leverage and collaborate with security vendors and government resources to implement and improve security controls.

Private Sector Needs from Congress and the Administration

Dow believes that protection of the country's critical infrastructure can be addressed most effectively by moving forward with legislation which strengthens the collaboration between the public and the private sectors. This collaboration must

recognize the benefits of a risk based and performance based approach, its relationship to physical security, two-way information sharing, prosecution of cyber criminals and protection from liability. This should be done in a way that does not impact the relationships developed over the last decade.

Effective two-way cyber security information sharing between the public and private sectors must be timely, specific and actionable, and protected from public disclosure. A public/private partnership will vastly improve the flow of information and ideas to quickly identify threats and vulnerabilities. To help promote the flow of information, information voluntarily provided by the private sector should be adequately protected from public disclosure. The unintended consequences of Freedom of Information Act requests must be addressed.

Liability protection for the private sector as a result of a cyber attack must also be provided as long as appropriate management systems have been applied to address potential threats. This will help promote participation amid the more rapid penetration of emerging technologies. The liability protections afforded under the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 are appropriate to consider.

Companies such as Dow are in a defensive mode when it comes to cybercrime. There must be better enforcement of U.S. laws against cybercrime with more aggressive prosecution of cyber criminals in an attempt to deter the act. U.S. laws should be updated and strengthened to protect critical infrastructure from cyber attacks and hold those accountable for perpetrating intentional acts designed to cause harm to critical infrastructure operating systems or for stealing intellectual property and personal information for financial gain. Additionally, the U.S. Federal Government should develop strong international partnerships that work together to identify international threats. Without a focused strategy to address the borderless nature of cybercrime, the private sector will continue to fight an uphill battle.

Dow believes the Federal Government has a role in setting an example, by ensuring higher quality security-embedded solutions and services by technology suppliers are built into their systems. Suppliers of IT products and services are best positioned to address issues within the solutions they create and have a responsibility to test and enhance product security, to understand their vulnerability before releasing items into the marketplace. Information technology suppliers and software developers must design for critical infrastructure high-availability and long-lived assets in accordance with rigorous compliance standards. The IT industry is in the best position to enhance security controls. If they do not, it passes an additional burden downstream, and duplicates effort and costs onto the customers in regulated industries. Just as the chemical sector adopted the Responsible Care model, the IT and telecommunication industries must be encouraged by their customer based to create self-regulated security practices and services.

Legislation

Dow advocates for legislation that codifies the principles outlined above. In summary, legislation that facilitates information sharing between industry and government and among industry peers is needed. Ideal information sharing legislation offers liability protections for early sharing threat or attack information with the government and provides antitrust relief to share with industry peers. Information should include strategic assessments, best practices, and lessons learned from events and incidents. Cyber criminals and nation state actors must not be allowed to continue to operate with relative impunity. They must believe that there are consequences for their actions. Finally, the IT and Telecommunications industries must create products which are inherently more secure.

Dow does not support prescriptive regulatory legislation on specific technologies or methods. Legislation that sets up a system requiring significant resources to simply comply with a regulatory scheme diverts resources from addressing the threats and risks in need of mitigation. Cyber security is a constantly changing portfolio and proper management requires a fluid and fast response. Complex regulatory schemes will only slow cyber risk management systems.

Executive Order on Improving Critical Infrastructure Cyber Security

Dow supports the information sharing initiatives included in the recent Executive order. However, Dow is concerned with the proposed approach of a voluntary program for critical infrastructure industries to adopt cybersecurity standards. Voluntary programs, normally, allow industry to develop their own standards that are risk and performance based that consider the specific sector environment, and are followed by a certification system to ensure compliance. Responsible Care Security code, for one, is a successful example for the Chemical sector.

Government defined or selected standards can miss the specific challenges that are required to be addressed by each industry sector. It is initiated as a voluntary program, but it could develop in such a way that companies will be forced to adopt prescriptive standards due to the fact that information on program adoption for "high risk" industries may be made public. More concerning this could be done without a review process and could be used to leverage in ways that may not be beneficial to lowering overall risk. The president or Congress should not allow pseudo-regulations without legislation to occur.

Dow will actively participate in industry forums like ACC, Chamber of Commerce, the Business Roundtable and all government initiatives to fully support successful implementation of any cyber security efforts which better protect our communities and industries.

Chairman ROCKEFELLER. Thank you, sir, very much.

Now we go to Greg Wilshusen.

STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Rockefeller, Chairman Carper, Ranking Member Coburn, Ranking Member Thune, and other members of the Committees, thank you very much for the opportunity to testify today at today's hearing on cybersecurity.

As you know, Federal agencies and our nation's critical infrastructures have become increasingly dependent on interconnected systems and networks that carry out essential operations. While creating significant benefits, this dependency also introduces vulnerabilities in cyber-based threats. These threats could have a potentially serious impact on Federal operations and essential services provided by the private sector.

Underscoring the importance of this issue, we have once again designated Federal information security and cyber-critical infrastructure protection as a governmentwide high-risk area. Today, I'll discuss the cyber threats confronting the private sector and Federal Government, several challenges to securing systems, and our assessment of the national cybersecurity strategy.

But, before I do, if I may, I'd like to recognize several of my colleagues who were instrumental in developing the body of work upon which my statement is based. Attending with me is Lee McCracken and Jeff Woodward, in the back, in the second row; in addition, Naba Barkakati, John de Ferrari, Rich Hung, Nicole Jarvis, and David Plocher made significant contributions.

Cyber-based threats to systems supporting critical infrastructure in Federal operations are evolving and growing. These threats come from a variety of sources, giving—including employees and other insiders, criminal groups, hackers, and foreign nations. These sources vary, in terms of their capabilities, willingness to act, and motives. The unique nature of cyber-based attacks can vastly enhance their reach and their impact. They can originate from around the globe and adversely affect economic and national security, and public health and safety.

Over the past 6 years, the number of cyber incidents reported by Federal agencies to US-CERT has increased from about 5500 in Fiscal Year 2006 to 48,562 in Fiscal Year 2012, an increase of 782 percent. These incidents, and the recently reported cyber-based attacks against businesses, further underscore the need to manage

and bolster the security of Federal systems and our nation's critical cyber assets.

However, the Federal Government continues to face challenges in effectively securing its systems and those supporting critical infrastructure. While actions have been taken to address aspects of these challenges, issues remain. A longstanding challenge has been designing and implementing risk-based information security programs at Federal agencies.

Another challenge has been establishing and identifying standards for critical infrastructures; and other challenges include detecting, responding to, and mitigating cyber incidents; securing the use of new technologies; and managing risk to the global IT supply chain.

Over the past 12 years, the Federal Government has identified a variety of documents that were intended to articulate a national cybersecurity strategy; however, it has not developed an overarching strategy that synthesizes the relevant portions of these documents or provides a comprehensive description of the current strategy. In addition, the strategy documents sometimes did not incorporate desirable characteristics that enhanced their usefulness. While the documents have generally included elements such as problem definition, goals, and subordinate objectives, they have not always fully addressed milestones and performance measures, cost and resource information, clearly defined roles and responsibilities, and linkage with other key strategy documents.

In our February 2013 report, we recommended that the White House cybersecurity coordinator develop an overarching cybersecurity strategy that addresses all key desirable characteristics and addresses cyber challenge areas.

Also last month, the President issued an Executive order on improving critical infrastructure cybersecurity. The Executive order includes actions aimed at addressing challenges in developing standards for critical infrastructure and sharing information. Although it is too soon to comment on its effectiveness, the order assigns specific responsibilities to specific individuals with specific deadlines; thus, providing clarity of responsibility and a means for establishing accountability.

In summary, addressing the ongoing challenges and implementing effective cybersecurity within the government, as well in collaboration with the private sector and other partners, requires the Federal Government to better define and more effectively implement an integrated national strategy that fully addresses key characteristics, provides a roadmap for resolving identified challenges, articulates a clear process for overseeing agency risk management, and assures accountability for results.

This concludes my statement. I'll be happy to answer any questions you may have.

[The prepared statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE

"Cybersecurity: A Better Defined and Implemented National Strategy is Needed to Address Persistent Challenges"

Chairmen Rockefeller and Carper, Ranking Members Thune and Coburn, and Members of the Committees:

Thank you for the opportunity to testify at today's hearing on the cybersecurity partnership between the private sector and our government.

As you know, with the advance of computer technology, Federal agencies and our nation's critical infrastructures—such as the electricity grid, water supply, telecommunications, and emergency services—have become increasingly dependent on computerized information systems and electronic data to carry out operations and process, maintain, and report essential information. While bringing significant benefits, this dependency can also create vulnerabilities to cyber-based threats. Pervasive and sustained cyber attacks against the United States could have a potentially serious impact on Federal and nonfederal systems and operations. Underscoring the importance of this issue, we have designated Federal information security as a high-risk area since 1997 and in 2003 expanded this area to include protecting computerized systems supporting our nation's critical infrastructure.[1]

Federal law and policy call for a risk-based approach to managing cybersecurity within the government and also specify activities to enhance the cybersecurity of public and private infrastructures that are essential to national security, economic security, and public health and safety. Over the last 12 years, the Federal Government has developed a number of strategies and plans for addressing cybersecurity based on this legal framework, including the *National Strategy to Secure Cyberspace,* issued in February 2003, and subsequent plans and strategies that address specific sectors, issues, and revised priorities.

In my testimony today, I will summarize (1) several challenges faced by the Federal Government in effectively implementing cybersecurity, including complying with the Federal Information Security Management Act, and (2) the extent to which the national cybersecurity strategy includes key desirable characteristics of effective strategies. My statement is based on our recently released report examining the Federal Government's cybersecurity strategies and the status of Federal efforts to address challenges in implementing cybersecurity,[2] as well as other previous work in this area. (Please see app. I for a list of related GAO products.)

The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Threats to systems supporting critical infrastructure and Federal information systems are evolving and growing. Advanced persistent threats—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives repeatedly over an extended period of time—pose increasing risks. In 2009, the President declared the cyber threat to be "[o]ne of the most serious economic and national security challenges we face as a nation" and stated that "America's economic prosperity in the 21st century will depend on cybersecurity."[3] The Director of National Intelligence has also warned of the increasing globalization of cyber attacks, including those carried out by foreign militaries or organized international crime. In January 2012, he testified that such threats pose a critical national and economic security concern.[4] To further highlight the importance of the threat, on October 11, 2012, the Secretary of Defense stated that the collective result of attacks

---

[1] See most recently, GAO, *High-Risk Series: An Update,* GAO–13–283 (Washington, D.C.: Feb. 14, 2013).

[2] GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented,* GAO–13–187 (Feb. 14, 2003).

[3] President Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure" (Washington, D.C.: May 29, 2009).

[4] James R. Clapper, Director of National Intelligence, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence" (January 31, 2012).

on our nation's critical infrastructure could be "a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life." [5]

The evolving array of cyber-based threats facing the nation pose threats to national security, commerce and intellectual property, and individuals. These threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources. These sources include business competitors, corrupt employees, criminal groups, hackers, and foreign nations engaged in espionage and information warfare. Such threat sources vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. Table 1 shows common sources of adversarial cybersecurity threats.

Table 1.—Sources of Adversarial Threats to Cybersecurity

Threat source	Description
Bot-network operators	Bot-network operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (*e.g.,* purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Business competitors	Companies that compete against or do business with a target company may seek to obtain sensitive information to improve their competitive advantage in various areas, such as pricing, manufacturing, product development, and contracting.
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
International corporate spies	International corporate spies pose a threat to the United States through their ability to conduct economic and industrial espionage [a] and large-scale monetary theft and to hire or develop hacker talent.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. In his January 2012 testimony, the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern.
Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware or malware to accomplish their objectives.
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (*e.g.,* a denial of service).

[5] Secretary of Defense Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City" (New York, NY: Oct. 11, 2012).

Table 1.—Sources of Adversarial Threats to Cybersecurity—Continued

Threat source	Description
Spyware or malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive viruses and worms have harmed files and hard drives, and reportedly have even caused physical damage to critical infrastructure, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, and Code Red.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center.

[a]According to the Office of the National Counterintelligence Executive, industrial espionage, or theft of trade secrets, occurs when an actor, intending or knowing that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner. See *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace.*

These sources of cybersecurity threats make use of various techniques to compromise information or adversely affect computers, software, a network, an organization's operation, an industry, or the Internet itself. Table 2 provides descriptions of common types of cyber attacks.

Table 2.—Common Types of Cyber Attacks

Types of attack	Description
Cross-site scripting	An attack that uses third-party web resources to run a script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Logic bombs	A piece of programming code intentionally inserted into a software system that will cause a malicious function to occur when one or more specified conditions are met.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Structured Query Language injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. Unlike a worm, a virus requires human involvement (usually unwitting) to propagate.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer– sometimes with a powerful antenna–searching for unsecured wireless networks.

Table 2.—Common Types of Cyber Attacks—Continued

Types of attack	Description
Worm	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. Unlike viruses, worms do not require human involvement to propagate.

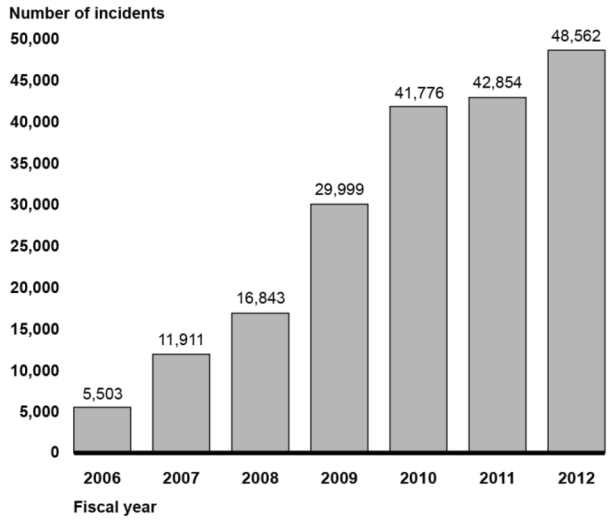
Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports.

The unique nature of cyber-based attacks can vastly enhance their reach and impact, resulting in the loss of sensitive information and damage to economic and national security, the loss of privacy, identity theft, and the compromise of proprietary information or intellectual property. The increasing number of incidents reported by Federal agencies, and the recently reported cyber-based attacks against individuals, businesses, critical infrastructures, and government organizations have further underscored the need to manage and bolster the cybersecurity of our government's information systems and our Nation's critical infrastructures.

Number of Cyber Incidents Reported by Federal Agencies Continues to Rise

The number of cyber incidents affecting computer systems and networks continues to rise. Over the past 6 years, the number of cyber incidents reported by Federal agencies to the U.S. Computer Emergency Readiness Team (US–CERT) has increased from 5,503 in Fiscal Year 2006 to 48,562 in Fiscal Year 2012, an increase of 782 percent (see fig. 1).

Figure 1: Incidents Reported to US-CERT, Fiscal Years 2006-2012

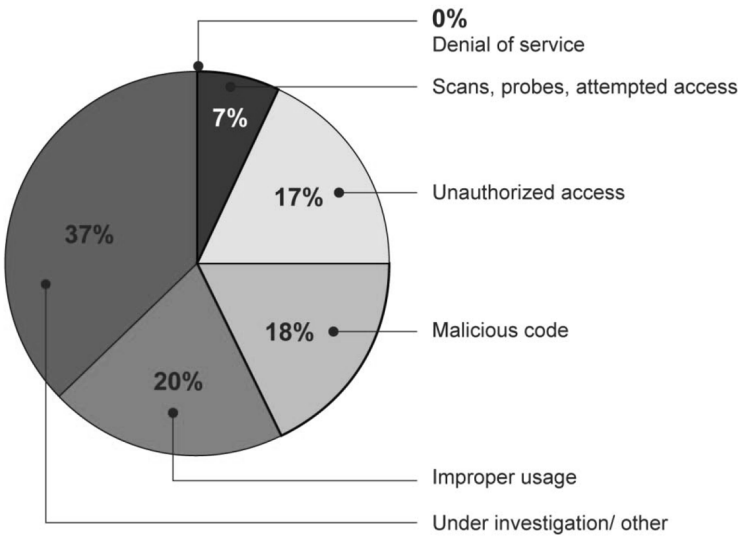


Source: GAO analysis of US–CERT data for fiscal years 2006–2012

Of the incidents occurring in 2012 (not including those that were reported as under investigation), improper usage,[6] malicious code, and unauthorized access were the most widely reported types across the Federal Government. As indicated in figure 2, which includes a breakout of incidents reported to US–CERT by agencies in Fiscal Year 2012, improper usage, malicious code, and unauthorized access accounted for 55 percent of total incidents reported by agencies.

[6] An incident is categorized as "improper usage" if a person violates acceptable computing use policies.

Figure 2: Incidents Reported to US-CERT by Federal Agencies in Fiscal Year 2012 by Category



Source: GAO analysis of US–CERT data for fiscal year 2012.

In addition, reports of cyber incidents affecting national security, intellectual property, and individuals have been widespread, with reported incidents involving data loss or theft, economic loss, computer intrusions, and privacy breaches. Such incidents illustrate the serious impact that cyber attacks can have on Federal and military operations; critical infrastructure; and the confidentiality, integrity, and availability of sensitive government, private sector, and personal information. For example, according to US–CERT, the number of agency-reported incidents involving personally identifiable information increased 111 percent from Fiscal Year 2009 to Fiscal Year 2012—from 10,481 to 22,156.

Federal Law and Policy Establish Information Security Responsibilities for Agencies

The Federal Government's information security responsibilities are established in law and policy. The Federal Information Security Management Act of 2002 (FISMA)[7] sets forth a comprehensive risk-based framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. In order to ensure the implementation of this framework, FISMA assigns specific responsibilities to agencies, the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and inspectors general:

- Each agency is required to develop, document, and implement an agency-wide information security program and to report annually to OMB, selected congressional committees, and the U.S. Comptroller General on the adequacy of its information security policies, procedures, practices, and compliance with requirements.
- OMB's responsibilities include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security in Federal agencies (except with regard to national security systems[8]). It is also respon-

[7] Title III of the E-Government Act of 2002, Pub. L. No. 107–347, Dec. 17, 2002; 44 U.S.C 3541, et seq.

[8] As defined in FISMA, the term "national security system" means any information system used by or on behalf of a Federal agency that (1) involves intelligence activities, national security-related cryptologic activities, command and control of military forces, or equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions (excluding systems used for routine administrative and business applications); or (2) is protected at all times by procedures established for handling classified national security information. See 44 U.S.C. §3542(b)(2).

sible for reviewing, at least annually, and approving or disapproving agency information security programs.

- NIST's responsibilities under FISMA include the development of security standards and guidelines for agencies that include standards for categorizing information and information systems according to ranges of risk levels, minimum security requirements for information and information systems in risk categories, guidelines for detection and handling of information security incidents, and guidelines for identifying an information system as a national security system.[9]
- Agency inspectors general are required to annually evaluate the information security program and practices of their agency. The results of these evaluations are to be submitted to OMB, and OMB is to summarize the results in its reporting to Congress.

In the 10 years since FISMA was enacted into law, Executive Branch oversight of agency information security has changed. As part of its FISMA oversight responsibilities, OMB has issued annual guidance to agencies on implementing FISMA requirements, including instructions for agency and inspector general reporting. However, in July 2010, the Director of OMB and the White House Cybersecurity Coordinator[10] issued a joint memorandum[11] stating that the Department of Homeland Security (DHS) was to exercise primary responsibility within the Executive Branch for the operational aspects of cybersecurity for Federal information systems that fall within the scope of FISMA.

The OMB memo also stated that in carrying out these responsibilities, DHS is to be subject to general OMB oversight in accordance with the provisions of FISMA. In addition, the memo stated that the Cybersecurity Coordinator would lead the interagency process for cybersecurity strategy and policy development. Subsequent to the issuance of M–10–28, DHS began issuing annual reporting instructions to agencies in addition to OMB's annual guidance.

Regarding Federal agencies operating national security systems, National Security Directive 42[12] established the Committee on National Security Systems, an organization chaired by the Department of Defense (DOD), to, among other things, issue policy directives and instructions that provide mandatory information security requirements for national security systems. In addition, the defense and intelligence communities develop implementing instructions and may add additional requirements where needed. An effort is underway to harmonize policies and guidance for national security and non-national security systems. Representatives from civilian, defense, and intelligence agencies established a joint task force in 2009, led by NIST and including senior leadership and subject matter experts from participating agencies, to publish common guidance for information systems security for national security and non-national security systems.[13]

Various laws and directives have also given Federal agencies responsibilities relating to the protection of critical infrastructures, which are largely owned by private sector organizations. The Homeland Security Act of 2002 created the Department of Homeland Security. Among other things, DHS was assigned with the following critical infrastructure protection responsibilities: (1) developing a comprehensive national plan for securing the critical infrastructures of the United States, (2) recommending measures to protect those critical infrastructures in coordination with other groups, and (3) disseminating, as appropriate, information to assist in the deterrence, prevention, and preemption of, or response to, terrorist attacks.

Homeland Security Presidential Directive 7 (HSPD–7) was issued in December 2003 and defined additional responsibilities for DHS, sector-specific agencies, and other departments and agencies. The directive instructed sector-specific agencies to collaborate with the private sector to identify, prioritize, and coordinate the protec-

---

[9] FISMA limits NIST to developing, in conjunction with the Department of Defense and the National Security Agency, guidelines for agencies on identifying an information system as a national security system, and for ensuring that NIST standards and guidelines are complementary with standards and guidelines developed for national security systems.

[10] In December 2009, a Special Assistant to the President was appointed as Cybersecurity Coordinator to address the recommendations made in the Obama administration's 2009 *Cyberspace Policy Review.*

[11] OMB, Memorandum M–10–28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security* (Washington, D.C.: July 6, 2010).

[12] National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (July 5, 1990).

[13] See GAO, *Information Security: Progress Made in Harmonizing Policies and Guidance for National Security and Non-National Security Systems,* GAO 10 916 (Washington, D.C.: Sept. 15, 2010).

tion of critical infrastructures to prevent, deter, and mitigate the effects of attacks. It also made DHS responsible for, among other things, coordinating national critical infrastructure protection efforts and establishing uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors.

On February 12, 2013, the President issued an executive order on improving the cybersecurity of critical infrastructure.[14] Among other things, it stated that the policy of the U.S. government is to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities and ordered the following actions to be taken:

- The Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence are, within 120 days of the date of the order, to issue instructions for producing unclassified reports of cyber threats and establish a process for disseminating these reports to targeted entities.
- Agencies are to coordinate their activities under the order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. In addition, DHS's Chief Privacy Officer and Officer for Civil Rights and Civil Liberties are to assess the privacy and civil liberties risks and recommend ways to minimize or mitigate such risks in a publicly available report to be released with 1 year of the date of the order.
- The Secretary of Homeland Security is to establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure.
- The Secretary of Commerce is to direct the Director of NIST to lead the development of a framework to reduce cyber risks to critical infrastructure. The framework is to include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks and incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Director is to publish a preliminary version of the framework within 240 days of the date of the order, and a final version within 1 year.
- The Secretary of Homeland Security, in coordination with sector-specific agencies, is to establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities. Further, the Secretary is to coordinate the establishment of a set of incentives designed to promote participation in the program and, along with the Secretaries of the Treasury and Commerce, make recommendations to the President that include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities.
- The Secretary of Homeland Security, within 150 days of the date of the order, is to use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.
- Agencies with responsibilities for regulating the security of critical infrastructure are to consult with DHS, OMB, and the National Security Staff to review the preliminary cybersecurity framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. If current regulatory requirements are deemed to be insufficient, agencies are to propose actions to mitigate cyber risk, as appropriate, within 90 days of publication of the final Cybersecurity Framework. In addition, within 2 years after publication of the final framework, these agencies, in consultation with owners and operators of critical infrastructure, are to report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements.

Also on February 12, 2013, the White House released Presidential Policy Directive (PPD) 21, on critical infrastructure security and resilience.[15] This directive revokes HSPD–7, although it states that plans developed pursuant to HSPD–7 shall remain in effect until specifically revoked or superseded. PPD–21 sets forth roles and re-

[14] Exec. Order No. 13636, 78 Fed. Reg. 11737 (Feb. 19, 2013). The order is also available at *http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.*

[15] The White House, Presidential Policy Directive/PPD–21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013), *http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.*

sponsibilities for DHS, sector-specific agencies, and other Federal entities with regard to the protection of critical infrastructure from physical and cyber threats. It also identifies three strategic imperatives to refine and clarify functional relationships across the Federal Government (which includes two national critical infrastructures centers for physical and cyber infrastructure), enable efficient information exchange by identifying baseline data and systems requirements, and implement an integration and analysis function to inform planning and operational decisions.

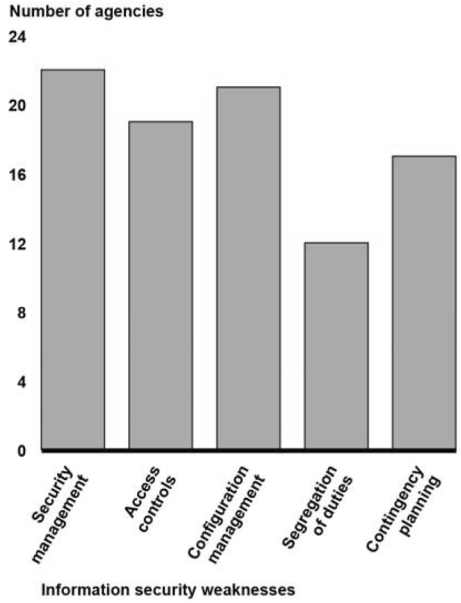
The directive calls for a number of specific implementation actions, along with associated time frames, which include developing a description of the functional relationships within DHS and across the Federal Government related to critical infrastructure security and resilience; conducting an analysis of the existing public-private partnership model; identifying baseline data and system requirements for the efficient exchange of information and intelligence; demonstrating a near real-time situational awareness capability for critical infrastructure; updating the National Infrastructure Protection Plan; and developing a national critical infrastructure security and resilience research and development plan. Finally, the directive identifies 16 critical infrastructure sectors and their designated Federal sector-specific agencies.

The Federal Government Continues to Face Challenges in Effectively Implementing Cybersecurity

We and Federal agency inspector general reports have identified challenges in a number of key areas of the Federal Government's approach to cybersecurity, including those related to protecting the Nation's critical infrastructure. While actions have been taken to address aspects of these challenges, issues remain in each of the following areas.

Designing and implementing risk-based cybersecurity programs at Federal agencies. Shortcomings persist in assessing risks, developing and implementing security controls, and monitoring results at Federal agencies. Specifically, for Fiscal Year 2012, 19 of 24 major Federal agencies reported that information security control deficiencies were either a material weakness or significant deficiency in internal controls over financial reporting. Further, inspectors general at 22 of 24 agencies cited information security as a major management challenge for their agency. Most of the 24 major agencies had information security weaknesses in most of five key control categories: implementing agency-wide information security management programs that are critical to identifying control deficiencies, resolving problems, and managing risks on an ongoing basis; limiting, preventing, and detecting inappropriate access to computer resources; managing the configuration of software and hardware; segregating duties to ensure that a single individual does not control all key aspects of a computer-related operation; and planning for continuity of operations in the event of a disaster or disruption (see fig. 3).

Figure 3: Information Security Weaknesses at 24 Major Agencies in Fiscal Year 2012



Source: GAO analysis of agency, inspectors general, and GAO reports as of December 13, 2012.

As we noted in our October 2011 report on agencies' implementation of FISMA requirements, an underlying reason for these weaknesses is that agencies have not fully implemented their information security programs.[16] As a result, they have limited assurance that controls are in place and operating as intended to protect their information resources, thereby leaving them vulnerable to attack or compromise. Accordingly, we have continued to make numerous recommendations to address specific weaknesses in risk management processes at individual Federal agencies. Recently, some agencies have demonstrated improvement in this area. For example, we reported in November 2012 that during Fiscal Year 2012, the Internal Revenue Service (IRS) continued to make important progress in addressing numerous deficiencies in its information security controls over its financial reporting systems.[17] Nonetheless, applying effective controls over agency information and information systems remains an area of significant concern.

Establishing and identifying standards for critical infrastructures. As we reported in December 2011, DHS and other agencies with responsibilities for specific critical infrastructure sectors have not yet identified cybersecurity guidance applicable to or widely used in each of the sectors.[18] Moreover, sectors vary in the extent to which they are required by law or regulation to comply with specific cybersecurity requirements. Within the energy sector, for example, experts have identified a lack of clarity in the division of responsibility between Federal and state regulators as a challenge in securing the U.S. electricity grid. We have made recommendations aimed at furthering efforts by sector-specific agencies to enhance critical infrastructure protection. The recently issued executive order is also intended to bolster efforts in this challenge area.

Detecting, responding to, and mitigating cyber incidents. DHS has made progress in coordinating the Federal response to cyber incidents, but challenges remain in

[16] GAO, *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements,* GAO–12–137 (Washington, D.C.: Oct. 3, 2011).

[17] GAO, *Financial Audit: IRS's Fiscal Years 2012 and 2011 Financial Statements,* GAO–13–120 (Washington, D.C.: Nov. 9, 2012).

[18] GAO, *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use,* GAO–12–92 (Washington, D.C.: Dec. 9, 2011).

sharing information among Federal agencies and key private-sector entities, including critical infrastructure owners. Difficulties in sharing information and the lack of a centralized information-sharing system continue to hinder progress. The February executive order contains provisions aimed at addressing these difficulties by, for example, establishing a process for disseminating unclassified reports of threat information. Challenges also persist in developing a timely cyber analysis and warning capability. While DHS has taken steps to establish a timely analysis and warning capability, we have reported that it had yet to establish a predictive analysis capability and recommended that the department establish such capabilities.[19] According to DHS, tools for predictive analysis are to be tested in Fiscal Year 2013.

Promoting education, awareness, and workforce planning. In November 2011, we reported that Federal agencies leading strategic planning efforts for cybersecurity education and awareness had not identified details for achieving planned outcomes and that specific tasks and responsibilities were unclear.[20] We recommended, among other things, that these agencies collaborate to clarify responsibilities and processes for planning and monitoring their activities. We also reported that only two of eight agencies in our review had developed cyber workforce plans, and only three of the eight agencies had a department-wide training program for their cybersecurity workforce. We recommended that these agencies take steps to improve agency and government-wide cybersecurity workforce efforts. Agencies concurred with the majority of our recommendations and outlined steps to address them.

Supporting cyber research and development. The support of targeted cyber research and development (R&D) has been impeded by implementation challenges among Federal agencies. In June 2010, we reported that R&D initiatives were hindered by limited sharing of detailed information about ongoing research, including the lack of a process for sharing results of completed projects or a repository to track R&D projects funded by the Federal Government.[21] To help facilitate information sharing about planned and ongoing R&D projects, we recommended establishing a mechanism for tracking ongoing and completed Federal cybersecurity R&D projects and their funding, and that this mechanism be used to develop an ongoing process to share R&D information among Federal agencies and the private sector. As of September 2012, this mechanism had not been fully developed.

Securing the use of new technologies. Addressing security concerns related to the use of emerging technologies such as cloud computing, social media, and mobile devices is a continuing challenge. In May 2010, we reported that Federal agencies had not taken adequate steps to ensure that security concerns were addressed in their use of cloud-based services, and made several recommendations to address cloud computing security, which agencies have begun to implement.[22] Further, we reported in June 2011 that Federal agencies did not always have adequate policies in place for managing and protecting information they access and disseminate through social media platforms such as Facebook and Twitter and recommended that agencies develop such policies.[23] Most of the agencies agreed with our recommendations. In September 2012, we reported that the U.S. Federal Communications Commission could do more to encourage mobile device manufacturers and wireless carriers to implement a more complete industry baseline of mobile security safeguards.[24] The commission generally concurred with our recommendations.

Managing risks to the global information technology supply chain. Reliance on a global supply chain for information technology products and services introduces risks to systems, and Federal agencies have not always addressed these risks. Specifically, in March 2012, we reported that four national security-related agencies varied in the extent to which they had defined supply chain protection measures for their information systems and were not in a position to develop implementing proce-

---

[19] GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability,* GAO–08–588 (Washington, D.C.: July 31, 2008).

[20] GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination,* GAO–12–8 (Washington, D.C.: Nov. 29, 2011).

[21] GAO, *Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development,* GAO–10–466 (June 3, 2010).

[22] GAO, *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing,* GAO–10–513 (Washington, D.C.: May 27, 2010).

[23] GAO, *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate,* GAO–11–605 (Washington, D.C.: June 28, 2011).

[24] GAO, *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged,* GAO–12–757 (Washington, D.C.: Sept. 18, 2012).

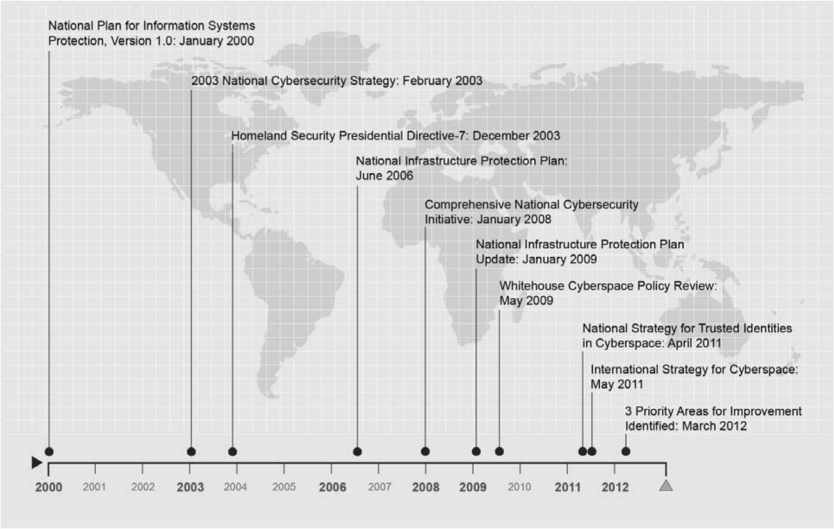
dures and monitoring capabilities for such measures.[25] We recommended that the agencies take steps as needed to address supply chain risks, and the departments generally concurred.

Addressing international cybersecurity challenges. While the Federal Government has identified the importance of international cooperation for cybersecurity and has assigned related roles and responsibilities to Federal agencies, its approach to addressing international aspects of cybersecurity has not been fully defined or implemented. We reported in July 2010 that the government faced a number of challenges in this area, relating to providing top-level leadership to coordinate actions among agencies, developing a national strategy, coordinating policy among key Federal entities, ensuring that international technical standards and policies do not impose unnecessary trade barriers, participating in international cyber-incident response efforts, investigating and prosecuting international cybercrime, and developing international models and norms for behavior.[26] We recommended that the government develop a global cyberspace strategy to help address these challenges. While such a strategy has been developed and includes goals such as the development of international cyberspace norms, it does not fully specify outcome-oriented performance metrics or timeframes for completing activities.

The U.S. National Cybersecurity Strategy Has Evolved over Time but Is Not Well Defined

The Federal Government has issued a variety of documents over the last decade that were intended to articulate a national cybersecurity strategy. The evolution of the Nation's cybersecurity strategy is summarized in figure 4.

Figure 4: Evolution of National Strategies Related to Cybersecurity



Source: GAO analysis of federal strategy documents.

These strategy documents address aspects of the above-mentioned challenge areas. For example, they address priorities for enhancing cybersecurity within the Federal Government as well as for encouraging improvements in the cybersecurity of critical infrastructures within the private sector.

However, as we noted in our February 2013 report, the government has not developed an overarching national cybersecurity strategy that synthesizes the relevant portions of these documents or provides a comprehensive description of the current strategy.[27] The Obama administration's 2009 *Cyberspace Policy Review* recommended a number of actions, including updating the 2003 *National Cybersecurity*

[25] GAO, *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks,* GAO–12–361 (Washington, D.C.: Mar. 23, 2012).

[26] GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance,* GAO–10–606 (Washington, D.C.: July 2, 2010).

[27] GAO–13–187.

Strategy. However, no updated strategy document has been issued. In May 2011, the White House announced that it had completed all the near-term actions outlined in the 2009 policy review, including the update to the 2003 national strategy. According to the administration's fact sheet on cybersecurity accomplishments,[28] the 2009 policy review itself serves as the updated strategy. The fact sheet stated that the direction and needs highlighted in the *Cyberspace Policy Review* and the previous national cybersecurity strategy were still relevant, and it noted that the administration had updated its strategy on two subordinate cyber issues, identity management and international engagement. Nonetheless, these actions do not fulfill the recommendation that an updated strategy be prepared for the President's approval. As a result, no overarching strategy exists to show how the various goals and activities articulated in current documents form an integrated strategic approach.

In addition to lacking an integrated strategy, the government's current approach to cybersecurity lacks key desirable characteristics of a national strategy. In 2004, we developed a set of desirable characteristics that can enhance the usefulness of national strategies in allocating resources, defining policies, and helping to ensure accountability.[29] Table 3 summarizes these key desirable characteristics.

Table 3.—Desirable Characteristics for a National Strategy

Desirable characteristic	Description
Purpose, scope, and methodology	Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed.
Problem definition and risk assessment	Addresses the particular national problems and threats the strategy is directed toward.
Goals, subordinate objectives, activities, and performance measures	Addresses what the strategy is trying to achieve and steps to achieve those results, as well as the priorities, milestones, and performance measures to gauge results.
Resources, investments, and risk management	Addresses what implementation of the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted based on balancing risk reductions with costs.
Organizational roles, responsibilities, and coordination	Addresses who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.
Linkage to other strategies and implementation	Addresses how a national strategy relates to other strategies' goals, objectives, and activities, and to subordinate levels of government and their plans to implement the strategy.

Source: GAO.

Existing cybersecurity strategy documents have included selected elements of these desirable characteristics, such as setting goals and subordinate objectives, but have generally lacked other key elements. The missing elements include the following:

Milestones and performance measures. The government's strategy documents include few milestones or performance measures, making it difficult to track progress in accomplishing stated goals and objectives. This lack of milestones and performance measures at the strategic level is mirrored in similar shortcomings within key programs that are part of the government-wide strategy. For example, in 2011 the DHS inspector general recommended that the department develop and implement performance measures to track and evaluate the effectiveness of actions defined in its strategic plan,[30] which the department had yet to do as of January 2012.

Cost and resources. While past strategy documents linked certain activities to Federal agency budget requests, none have fully addressed cost and resources, including justifying the required investment, which is critical to gaining support for implementation. Specifically, none of the strategy documents provided full

[28] The White House, "Fact Sheet: The Administration's Cybersecurity Accomplishments" (May 12, 2011), accessed on July 26, 2012, *http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-administrations-cybersecurity-accomplishments.*

[29] See GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism,* GAO–04–408T (Washington, D.C.: Feb. 3, 2004).

[30] DHS, Office of Inspector General, *Planning, Management, and Systems Issues Hinder DHS' Efforts to Protect Cyberspace and the Nation's Cyber Infrastructure,* OIG–11–89 (Washington, D.C.: June 2011).

assessments of anticipated costs and how resources might be allocated to meet them.

Roles and responsibilities. Cybersecurity strategy documents have assigned high-level roles and responsibilities but have left important details unclear. Several GAO reports have likewise demonstrated that the roles and responsibilities of key agencies charged with protecting the cyber assets of the United States are inadequately defined. For example, the chartering directives for several offices within the Department of Defense assign overlapping roles and responsibilities for preparing for and responding to domestic cyber incidents. In an October 2012 report, we recommended that the department update its guidance on preparing for and responding to domestic cyber incidents to include a description of roles and responsibilities.[31] Further, in March 2010, we reported that agencies had overlapping and uncoordinated responsibilities within the Comprehensive National Cybersecurity Initiative and recommended that OMB better define roles and responsibilities for all key participants.[32]

In addition, while the law gives OMB responsibility for oversight of Federal information security, OMB transferred several of its oversight responsibilities to DHS. OMB officials stated that enlisting DHS to perform these responsibilities has allowed OMB to have more visibility into agencies' cybersecurity activities because of the additional resources and expertise provided by DHS. While OMB's decision to transfer these responsibilities is not consistent with FISMA, it may have had beneficial practical results, such as leveraging resources from DHS. Nonetheless, with these responsibilities now divided between the two organizations, it is remains unclear how they are to share oversight of individual departments and agencies. Additional legislation could clarify these responsibilities.

Linkage with other key strategy documents. Existing cybersecurity strategy documents vary in terms of priorities and structure, and do not specify how they link to or supersede other documents. Nor do they describe how they fit into an overarching national cybersecurity strategy. For example, in 2012, the Obama administration identified three cross-agency cybersecurity priorities, but no explanation was given as to how these priorities related to those established in other strategy documents.

Actions Needed to Ensure More Effective Implementation of Cybersecurity

Given the range and sophistication of the threats and potential exploits that confront government agencies and the Nation's cyber critical infrastructure, it is critical that the government adopt a comprehensive strategic approach to mitigating the risks of successful cybersecurity attacks. In our February report, we recommended that the White House Cybersecurity Coordinator develop an overarching Federal cybersecurity strategy that includes all key elements of the desirable characteristics of a national strategy.[33] Such a strategy, we believe, will provide a more effective framework for implementing cybersecurity activities and better ensure that such activities will lead to progress in securing systems and information. This strategy should also better ensure that Federal Government departments and agencies are held accountable for making significant improvements in cybersecurity challenge areas by, among other things, clarifying how oversight will be carried out by OMB and other Federal entities. In the absence of such an integrated strategy, the documents that comprise the government's current strategic approach are of limited value as a tool for mobilizing actions to mitigate the most serious threats facing the Nation.

In addition, many of the recommendations previously made by us and agency inspectors general have not yet been fully addressed, leaving much room for more progress in addressing cybersecurity challenges. In many cases, the causes of these challenges are closely related to the key elements that are missing from the government's cybersecurity strategy. For example, the persistence of shortcomings in agency cybersecurity risk management processes indicates that agencies have not been held accountable for effectively implementing such processes and that oversight mechanisms have not been clear. It is just such oversight and accountability that is poorly defined in cybersecurity strategy documents.

---

[31] GAO, *Homeland Defense: DOD Needs to Address Gaps in Homeland Defense and Civil Support Guidance,* GAO–13–128 (Washington, D.C.: Oct. 24, 2012).

[32] GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative,* GAO–10–338 (Washington, D.C.: Mar. 5, 2010).

[33] GAO–13–187.

In light of this limited oversight and accountability, we also stated in our report that Congress should consider legislation to better define roles and responsibilities for implementing and overseeing Federal information security programs and protecting the Nation's critical cyber assets. Such legislation could clarify the respective responsibilities of OMB and DHS, as well as those of other key Federal departments and agencies.

In commenting on a draft of the report, the Executive Office of the President agreed that more needs to be done to develop a coherent and comprehensive strategy on cybersecurity but did not believe producing another strategy document would be beneficial. Specifically, the office stated that remaining flexible and focusing on achieving measurable improvements in cybersecurity would be more beneficial than developing "yet another strategy on top of existing strategies." We agree that flexibility and a focus on achieving measurable improvements in cybersecurity is critically important and that simply preparing another document, if not integrated with previous documents, would not be helpful. The focus of our recommendation is to develop an overarching strategy that integrates the numerous strategy documents, establishes milestones and performance measures, and better ensures that Federal departments and agencies are held accountable for making significant improvements in cybersecurity challenge areas. The Executive Office of the President also agreed that Congress should consider enhanced cybersecurity legislation that addresses information sharing and baseline standards for critical infrastructure, among other things.

In summary, addressing the ongoing challenges in implementing effective cybersecurity within the government, as well as in collaboration with the private sector and other partners, requires the Federal Government to define and implement a coherent and comprehensive national strategy that includes key desirable elements and provides accountability for results. Recent efforts, such as the 2012 cross-agency priorities and the executive order on improving cybersecurity for critical infrastructure, could provide parts of a strategic approach. For example, the executive order includes actions aimed at addressing challenges in developing standards for critical infrastructure and sharing information, in addition to assigning specific responsibilities to specific individuals that are to be completed within specific timeframes, thus providing clarity of responsibility and a means for establishing accountability. However, these efforts need to be integrated into an overarching strategy that includes a clearer process for oversight of agency risk management and a roadmap for improving the cybersecurity challenge areas in order for the government to make significant progress in furthering its strategic goals and lessening persistent weaknesses.

Chairmen Rockefeller and Carper, Ranking Members Thune and Coburn, and Members of the Committees, this concludes my statement. I would be happy to answer any questions you may have.

GAO Contacts and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen (*wilshuseng@gao.gov*) or Dr. Nabajyoti Barkakati (*barkakatin@gao.gov*). Other key contributors to this statement include John de Ferrari (Assistant Director), Richard B. Hung (Assistant Director), Nicole Jarvis, Lee McCracken, David F. Plocher, and Jeffrey Woodward.

APPENDIX I: RELATED GAO PRODUCTS

Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. GAO–13–187. Washington, D.C.: February 14, 2013.

High-Risk Series: An Update. GAO–13–283. Washington, D.C.: February 14, 2013.

*Information Security: Federal Communications Commission Needs to Strengthen Controls over Enhanced Secured Network Projec*t. GAO–13–155. Washington, D.C.: January 25, 2013.

Information Security: Actions Needed by Census Bureau to Address Weaknesses. GAO–13–63. Washington, D.C.: January 22, 2013.

Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged. GAO–12–757. Washington, D.C.: September 18, 2012.

Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy. GAO–12–903. Washington, D.C.: September 11, 2012.

Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices. GAO–12–816. August 31, 2012.

Cybersecurity: Challenges in Securing the Electricity Grid. GAO–12–926T. Washington, D.C.: July 17, 2012.

Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight. GAO–12–479. Washington, D.C.: July 9, 2012.

Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage. GAO–12–876T. Washington, D.C.: June 28, 2012.

Cybersecurity: Threats Impacting the Nation. GAO–12–666T. Washington, D.C.: April 24, 2012.

IT Supply Chain: National Security-Related Agencies Need to Better Address Risks. GAO–12–361. Washington, D.C.: March 23, 2012.

Information Security: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data. GAO–12–393. Washington, D.C.: March 16, 2012.

Cybersecurity: Challenges in Securing the Modernized Electricity Grid. GAO–12–507T. Washington, D.C.: February 28, 2012.

Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use. GAO–12–92. Washington, D.C.: December 9, 2011.

Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination. GAO–12–8. Washington, D.C.: November 29, 2011.

Information Security: Additional Guidance Needed to Address Cloud Computing Concerns. GAO–12–130T. Washington, D.C.: October 6, 2011.

Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements. GAO–12–137. Washington, D.C.: October 3, 2011.

Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards. GAO–11–751. Washington, D.C.: September 20, 2011.

Information Security: FDIC Has Made Progress, but Further Actions Are Needed to Protect Financial Data. GAO–11–708. Washington, D.C.: August 12, 2011.

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure. GAO–11–865T. Washington, D.C.: July 26, 2011.

Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities. GAO–11–75. Washington, D.C.: July 25, 2011.

Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain. GAO–11–149. Washington, D.C.: July 8, 2011.

Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate. GAO–11–605. Washington, D.C.: June 28, 2011.

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems. GAO–11–463T. Washington, D.C.: March 16, 2011.

Information Security: IRS Needs to Enhance Internal Control Over Financial Reporting and Taxpayer Data. GAO–11–308. Washington, D.C.: March 15, 2011.

Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to Be Addressed. GAO–11–117. Washington, D.C.: January 12, 2011.

Information Security: National Nuclear Security Administration Needs to Improve Contingency Planning for Its Classified Supercomputing Operations. GAO–11–67. Washington, D.C.: December 9, 2010.

Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk. GAO–11–43. Washington, D.C.: November 30, 2010.

Information Security: Federal Deposit Insurance Corporation Needs to Mitigate Control Weaknesses. GAO–11–29. Washington, D.C.: November 30, 2010.

Information Security: National Archives and Records Administration Needs to Implement Key Program Elements and Controls. GAO–11–20. Washington, D.C.: October 21, 2010.

Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed. GAO–11–24. Washington, D.C.: October 6, 2010.

Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems. GAO–10–916. Washington, D.C.: September 15, 2010.

Information Management: Challenges in Federal Agencies' Use of Web 2.0 Technologies. GAO–10–872T. Washington, D.C.: July 22, 2010.

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. GAO–10–628. Washington, D.C.: July 15, 2010.

Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. GAO–10–606. Washington, D.C.: July 2, 2010.

Information Security: Governmentwide Guidance Needed to Assist Agencies in Implementing Cloud Computing. GAO–10–855T. Washington, D.C.: July 1, 2010.

Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats. GAO–10–834T. Washington, D.C.: June 16, 2010.

Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development. GAO–10–466. Washington, D.C.: June 3, 2010.

Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing. GAO–10–513. Washington, D.C.: May 27, 2010.

Information Security: Opportunities Exist for the Federal Housing Finance Agency to Improve Control. GAO–10–528. Washington, D.C.: April 30, 2010.

Information Security: Concerted Response Needed to Resolve Persistent Weaknesses. GAO–10–536T.Washington, D.C.: March 24, 2010.

Information Security: IRS Needs to Continue to Address Significant Weaknesses. GAO–10–355. Washington, D.C.: March 19, 2010.

Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies. GAO–10–237. Washington, D.C.: March 12, 2010.

Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements. GAO–10–202. Washington, D.C.: March 12, 2010.

Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative. GAO–10–338. Washington, D.C.: March 5, 2010.

Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience. GAO–10–296. Washington, D.C.: March 5, 2010.

Department of Veterans Affairs' Implementation of Information Security Education Assistance Program. GAO–10–170R. Washington, D.C.: December 18, 2009.

Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats. GAO–10–230T. Washington, D.C.: November 17, 2009.

Information Security: Concerted Effort Needed to Improve Federal Performance Measures. GAO–10–159T. Washington, D.C.: October 29, 2009.

Critical Infrastructure Protection: OMB Leadership Needed to Strengthen Agency Planning Efforts to Protect Federal Cyber Assets. GAO–10–148. Washington, D.C.: October 15, 2009.

Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks. GAO–10–4. Washington, D.C.: October 15, 2009.

Information Security: Actions Needed to Better Manage, Protect, and Sustain Improvements to Los Alamos National Laboratory's Classified Computer Network. GAO–10–28. Washington, D.C.: October 14, 2009.

Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment. GAO–09–969. Washington, D.C.: September 24, 2009.

Information Security: Federal Information Security Issues. GAO–09–817R. Washington, D.C.: June 30, 2009.

Information Security: Concerted Effort Needed to Improve Federal Performance Measures. GAO–09–617. Washington, D.C.: September 14, 2009.

Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses. GAO–09–546. Washington, D.C.: July 17, 2009.

National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. GAO–09–432T. Washington, D.C.: March 10, 2009.

Information Technology: Federal Laws, Regulations, and Mandatory Standards to Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors. GAO–08–1075R. Washington, D.C.: September 16, 2008.

Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability. GAO–08–588. Washington, D.C.: July 31, 2008.

Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains. GAO–08–525. Washington, D.C.: June 27, 2008.

Privacy: Lessons Learned about Data Breach Notification. GAO–07–657. Washington, D.C.: April 30, 2007.

Chairman ROCKEFELLER. Thank you very much.

This could be to either of you, or both of you. And this is on the question of what I consider a desperately bad situation, in terms of trained work force, for cybersecurity across the nation.

I was with a business executive, who's a very good friend of mine, whose company I know very well, and he came in to see me, not about this subject, but about what his company had a concern about. And I asked him, "So, how are you fixed to take care of yourself on cybersecurity?" And he's, "We're fine." He said, "We're fine."

I don't want to be a psychiatrist, but I know him well enough—you can read body language, you can read voice inflection—and I really didn't believe that he meant to say that. I think he meant to say it, but I didn't believe it. There wasn't any demonstrated interest in it. His was one of the most vulnerable of all industries that could be affected by, you know, attacks—cyber attacks. And so, I didn't say anything about it, but I just—I noted, in my mind, that there was a lack of self-confidence, the lack of interest, and it wasn't believable. And, of course, I might have been absolutely wrong.

But, that just leads me to this question. There are so many huge things that we have to do in cybersecurity, but none of them come to anything unless there is a workforce out there which is trained, and trained to the specificity of everything from, you know, standards to what do you do about intellectual property—I mean, just the whole range. And, you know, sort of like when we were starting with the E-Rate or the Internet. I mean, people didn't know anything about it. They knew it was important, but they didn't know anything about it. Then, gradually, that took hold.

What, in your mind, should be done to get our country up to speed on training cybersecurity workforce?

Mr. WILSHUSEN. Well, I guess I'll take first stab at it. I think you're absolutely correct, this is an issue for the nation and certainly for the Federal workforce. We did a review and issued a report, last year, on human-capital workforce issues as it relates to cybersecurity. We did work at several agencies. One of the key themes that we identified is that, while agencies were generally able to fill many of their information security positions, they had the most challenge in identifying those individuals that had the technical skills in order to effectively implement security at a technical level.

There are a couple of initiatives underway that are intended to help improve the cyber workforce, to ensure better training of individuals, as well as to improve societal knowledge of cybersecurity, beginning early on, through K–12 and onward. One of them is the National Initiative for Cybersecurity Education that's run by DHS and NIST, who are key partners in that particular effort.

Chairman ROCKEFELLER. So, they put it into early curriculum.

Mr. WILSHUSEN. Yes. And that's one of the areas where the younger generation's probably more technically literate than I was at that time, and include it in curriculum early on, and carry throughout their education.

And then, within the Federal workforce, make sure we have the appropriate technical training and expertise that we can develop and grow our own workforce to address the cybersecurity challenges of today.

Chairman ROCKEFELLER. OK. Well, the Feds are part of it, private sector is another part of it.

Mr. KEPLER. Yes. What I would say is, when you look at the force we've had to put in our company, it's very technically-oriented, in terms of engineers, computer scientists. And I think the key thing the country needs to do, in general, is still foster the development of that kind of capability. And we're short of that, not only cybersecurity, but in a lot of the aspects of the science and technology that we need, to compete globally.

I think some of the early challenges has been that people have addressed this as purely an enforcement issue, and so the basis has been more security oriented than the technology underlying in content. And so, it's a mix of people who have thought about this from an enforcement point of view.

But, I think the general view of—the skills are going to change over time; they change, year over year, what we have to address. So, having grounded background in computer technology, in science and math, these are the things that you need to get people to work on to solve these problems. But, I think the company—or, country can do well, invested in that in a lot of different aspects of our prosperity.

Chairman ROCKEFELLER. So, if you do everything you want to do, how many years will it take for Dow, which is, obviously, one of the most sophisticated companies in the country, to get to where you want to be on work force security?

Mr. KEPLER. With work—I think we can hire the—you know, with paying a premium for that. We have almost 150 people, now, between direct people and contractors, that work in this space. It's getting the workforce for, actually, the next generation and the next decade to compete and work in our plants and our laboratories. And I think that's a critical issue for the government that's going to take a decade to address, Senator.

Chairman ROCKEFELLER. Which is where we've got to educate——

Mr. KEPLER. Yes.

Chairman ROCKEFELLER.—how dangerous this is.

Thank you.

Mr. Chairman.

Chairman CARPER. Thanks. Thanks, Senator Rockefeller.

Mr. Wilshusen, Senator Coburn suggested you'd be a good witness, and, boy, he was right.

And, Mr. Kepler, I think you may have been invited by Senator Thune, as I understand it, and we thank him for inviting you, and you for coming. We're honored, in Delaware, that Dow has a significant presence in our state, and think of you as a—we're fortunate to have you as one of our corporate citizens.

I think the first question I'm going to ask would be for either of them, but maybe we start with Mr. Wilshusen, if I could.

You have a disadvantage, you and the colleagues that you recognize. Not necessarily—not everybody recognizes the team that

helped put together an effort, and I know a lot of people were involved in this; we've got great people at GAO, and we thank you for all that you all do to help us do our jobs—but, had the disadvantage of preparing your report, which you released recently, before the administration, sort of, showed their hand on the Executive order. And just—if you had known what the Executive order was going to look like, and maybe had the benefit of this kind of testimony from the Secretary and from Mr. Gallagher, what would you have—how would your report have changed, if at all? I think it might have changed some, but your—in your testimony today, how might it have changed a bit?

Mr. WILSHUSEN. Well, actually I don't know if our report would change much, other than to identify the Executive order as another strategy-related document that has been developed by the administration. The Executive order certainly addresses one of the key challenge areas that we have identified in the past, in terms of identifying and establishing standards for cybersecurity in the critical infrastructures. And it also will help, in terms of another challenge, as it relates to providing and sharing information to, particularly, those in the private sector.

But, it's part of an overall strategy, though. It's still, like other strategy documents, focused on just one component of an overall national strategy. We still believe that the White House cybersecurity coordinator should develop an overarching strategy that integrates this Executive order with the other strategies.

One of the positive things that we noted with the Executive order is that it does assign specific responsibilities to individuals. And that's a plus. It also gives them specific deadlines in order to perform those activities. That's another plus. But, it still remains to be seen, in terms of the extent to which there's follow through to make sure that those activities are implemented, and implemented effectively.

Chairman CARPER. OK. Well, my hope is, before we're done, and we have done our job on the legislative side, that—or, you put the two together, what the administration has laid out and suggested and what we have done, hopefully, in response, to kind of fill out the package—that you'll say, "Yes, that's a pretty good strategy, and now the key is to implement it well."

If I could, Mr. Kepler, the—I think you mentioned the word "protection," the kind of—you or maybe one of our earlier witnesses talked about the kind of protections that—whether it's the chemical industry, whether it's other segments of our business industry, that they're looking for needing—I asked Secretary Napolitano about liability—punitive, general, other kinds of liability protection. She mentioned that there's more than just liability that can be afforded as an incentive or a protection for the—for industry. She mentioned—oh, gosh, I think she might have mentioned security—you know, expedited security clearances, so more information would be available to our key stakeholders.

Talk about what—the kind of protection that Dow or others in the chemical industry are looking for, and that they need in order to feel more comfortable with what you're being invited to participate in.

Mr. KEPLER. Yes. And I would make the point that I think the information protection goes both ways. I think one of the things that we would look at over the years is, we'd build up a technology base and, I think, a reasonable operating system base, but the key thing to make this all work is, you need competitive intelligence. And we get very little of that, and we don't have the resources or structure to make that happen. And so, the ability to get government to feel comfortable to share, with industry, specific areas that we can address, so we can get focused, is a critical issue.

So, I think if you contemplate legislation, it should think about it in both ways.

I think there are issues, when we go across on—not only on liability, but the concerns, sometimes, of sharing information on antitrust, and that the—when companies get to start to share information when there's an incident or an issue, and it gets into shipments or it gets into some other areas, how to make sure that we can manage those type of issues in that, as well.

So, I think the view of liability, you know, in our view, is that there—early on, within physical, but it actually can apply to cyber—there's the SAFETY Act that allowed—if you had a good management system in place, that was reviewed, you could actually get liability coverage on that. And we've submitted that, and actually are—fall under that Act, for us.

Chairman CARPER. Good. Thank you.

My thanks to you both.

Senator Thune.

Senator THUNE. Thank you, Mr. Chairman.

The GAO's recent report—of course, already talked about—highlighted some of the persistent shortcomings of the Federal Government's management of its own cybersecurity, which, I think, begs the question about them directing what the private sector should do.

And I want to go back, actually, to a 2010 report in which GAO reported that private-sector expectations are not being met for receiving usable cyber threat and cyber alert information from the government. For example, GAO reported that only 27 percent of private sector survey respondents were receiving actionable cyber threat information and alerts that met their expectations to a great or moderate extent. Of those receiving information, there were concerns that the information received is not tailored to each sector's needs, or the information does not have enough information to be useful.

So, my question—I would direct this, at least first, to you, Mr. Wilshusen—and that is, in what areas has the government made progress in sharing relevant information with the private sector? And do you have further recommendations?

Mr. WILSHUSEN. Yes, that's a good question. We have followed up on our recommendations made in that report, and we have found that DHS has started to implement a couple of them. But, it remains a challenge area. DHS has taken a number of steps. I know the Secretary, earlier, mentioned about the NCCIC, and that's one area in which it has started to improve the sharing of information through that mechanism.

I had also heard where the DHS has issued a relatively large number of security clearances, which can help facilitate the sharing of information.

But challenges still remain. We still find that, for example, it has not yet developed a predictive analysis capability, which would help lead to providing timely threat information, alert information, to private industry. And, as Mr. Kepler indicated in his prior remarks, it seems like that is still an area of improvement that can be made on the part of DHS and other Federal partners.

Senator THUNE. Mr. Kepler, do you feel you're receiving timely and usable cyber threat and cyber alert information from the government?

Mr. KEPLER. We don't receive content. I think we cooperate together, but there's a—we do not get specific information. And when we get attacked or get to a point that we can mitigate something, to try to go back and understand who it was and where it was and how we go address it in the future, that is rarely, if ever, given, and—or known, I don't know.

So, I'd say, you know, we talked about industrial espionage; there's clearly, from the government's viewpoint, I think, nation-sponsored espionage going on. I can't—I need the help of the government to address that. And so, that type of information, and how to deal with that collaboratively, we do not get.

Senator THUNE. Do you have any——

Mr. WILSHUSEN. And if I may——

Senator THUNE. Yes, go ahead.

Mr. WILSHUSEN. Excuse me. If I may just add one comment, too.

Senator THUNE. Yes.

Mr. WILSHUSEN. One of the elements that is probably missing is making sure that DHS or the Federal partners have a feedback mechanism, or a loop, where they can solicit and receive feedback from the private sector partners on how well they're doing in providing this type of information. It might be illuminating.

Senator THUNE. Yes.

If I might, too, Mr. Kepler, how important is information sharing peer-to-peer among others in the industry? And how's that working today? What's needed to improve it? Liability, antitrust protections, that sort of thing.

Mr. KEPLER. Yes, I would say that most of the industries that got stood up under its critical infrastructure have learned how to work together within their industries. The challenge is to start to work across industries. You know, obviously, if you look at cascading issues with power or with IT, it's to be able to share information. And I think the ability to bridge those stovepipes is the area that needs to be improved.

Senator THUNE. What's your biggest concern about the Executive order implementation process?

Mr. KEPLER. Well, I think there are two areas, as I pointed out. One concern is, to my—just a point, a minute ago—this is cascading. So, when you think about a significant failure, which is part of the risk that the Executive order is supposed to be—address, the—to me, the thing that we have to rely on is the IT suppliers and the government to have—to make sure that the communications networks work. And that seems to be—we're focusing

more downstream than upstream on what the fundamental issue is.

So, I hope, when we look at this, that most of the area needs to be around cyber in the infrastructure that we're building around the Internet and how that's being managed, because we all rely on that, including the government, to work on.

And the second thing I think—the standards has been talked a lot, but I think the viewpoint and transparency of how we're going to do risk assessment—because there's the gross risk of what could happen, but there's also understanding what's already been mitigated. So, I get concerned about how you develop the list of high-priority risks, to identify, to start to apply the resources you're going to apply. So, you can create an environment where you create a list of, kind of, generic issues and risk things, that we don't know how to get off that risk list. You know, we've been under CFATS and the physical side, and we've yet to get, you know, sites completely authorized, in terms of getting assessment against their authority. And so, you add cyber into that—I just think, in the next, you know, half a year to a year, to try to get all that risk assessment done, I think that's the area that we can have some unintended consequences in, Senator, unless we think through that clearly.

Senator THUNE. Thank you, Mr. Chairman.

Thank you very much.

Chairman CARPER. Dr. Coburn?

Senator COBURN. Well, let me follow up on that. You know, CFATS, as far as I'm concerned, so far, has been a failure. I don't know if that's your assessment to it, but we've spent billions of dollars, and we have very limited accomplishments there. It's not because we don't intend to. It's not. And cyber's five to six times more complex than that.

And one of the questions is, If DHS can't implement CFATS, and there hasn't been the same type of cooperative work upward, in terms of standards—in other words, one of the things—one of the great things about the Executive order is, the President did have his staff say, "Bring industry in, tell us what we need to do." In other words, there was upward communication from the people who actually know it. And that was somewhat lacking, in terms of the CFATS, and is still lacking, in my opinion.

So, do—given your experience on CFATS, what's your confidence level on DHS on cyber?

Mr. KEPLER. I guess that's my point.

Senator COBURN. Yes.

Mr. KEPLER. I think you look at CFATS as—the way it's laid out and put together, I think, is a sound thought process of how to work. So, we support the concept of CFATS. Do you have the right mindset to go—actually set standards and evaluate? Do you have the personnel to work on that?

So, I think the industry, as it relates to standards, the reality is, they're out there on cyber. We've worked a lot on process control systems, on management systems, on technology and networks. The previous panel described that.

The issue is, Are—Do we have a confident structure to evaluate those risks? And then do the assessment in government to collaborate with it. And I think that's where you need to improve.

So, my view has been, it's more an oversight issue than it is a legislation issue.

Senator COBURN. All right, thank you.

Mr. Wilshusen, I made, in my opening statement, a comment that we've not seen the report on FISMA. But, you all found that only 8 of 22 agencies are in compliance with that. And that's a decline from 13 agencies in 2010. What's the problem?

Mr. WILSHUSEN. We also are looking forward to receiving OMB's FISMA report. It usually provides a lot of useful information, particularly the portion where the IGs conduct their evaluations of their agency's information security programs. One of the issues that we have found over the years and why we have been designating Federal information security as a high-risk area since 1987 is because of agencies'—I won't say "inability," but their lack of meaningful success in securing their systems and meeting many of the requirements for securing their systems.

Senator COBURN. Let me explain——

Mr. WILSHUSEN. In your particular——

Senator COBURN. Let me explain what that means——

Mr. WILSHUSEN. Sure.

Senator COBURN.—so everybody understands. Only eight Federal agencies, at this time, out of 22, meet the guidelines for securing their network.

Mr. WILSHUSEN. And that's actually one of the statistics for assessing the risk——

Senator COBURN. Right.

Mr. WILSHUSEN.—which kind of gets to Mr. Kepler's point, in that it's one of the challenge areas for agencies. It's not an easy job, in terms of implementing effective security over time, because the environment is constantly changing, new technologies are being implemented into the computing environment, the threats are becoming more sophisticated, and business practices are changing.

But, at the same time, it's important that agencies implement the appropriate processes to assess their risk, and then, based on that risk, select the appropriate controls to cost-effectively reduce those risks to an acceptable level, and then assure that those controls are effectively implemented, tested, and remain appropriate over time.

If agencies don't assess their cyber risks appropriately at the very beginning and regularly thereafter, it has a cascading effect, in terms of the effectiveness of other controls.

Senator COBURN. Plus, it wastes a ton of money. You know, in the Federal Government, we spend $64 billion a year on IT, and, essentially, 50 percent of it is wasted, because we don't assess risks, and we don't contract appropriately.

Let me—in 2003, President Bush issued HSPD–7, which assigned several tasks to DHS pertaining to critical infrastructure and cybersecurity, including information sharing with the private sector—this was 2003; that's 10 years ago—and compiling a list of critical infrastructure.

The Executive order and the Presidential directive issued by the White House assigns DHS several tasks similar to those the agency was given in 2003. What's different?

Mr. WILSHUSEN. I think there are a couple of differences between the Executive order and HSPD–7. One is that HSPD–7 primarily focused on terrorist activities and counterterrorism; whereas, this particular Executive order is looking at a more broadbased threat factor, if you will, and to include resiliency and the like.

The other big difference here is that NIST is responsible—or has responsibility for creating the cybersecurity framework.

Senator COBURN. Yes. Actually, they're responsible for creating the standards, correct?

Mr. WILSHUSEN. Right. And——

Senator COBURN. The voluntary standards that are going to be maybe not so voluntary after they're created.

Mr. WILSHUSEN. Well, their label is a voluntary cybersecurity framework.

Senator COBURN. Yes.

Mr. WILSHUSEN. And I believe it's up to DHS and the sector-specific agencies to develop a program to help encourage adoption of that framework.

Senator COBURN. I'm over my time, Mr. Chairman, but I just——

I would like for you to make recommendations to Senator Carper and I, if you would, on what you would see as the best oversight function that we could have in looking how the Presidential directive and the Executive order is carried out. You know, this is a complex area. None of us are computer engineers or electrical engineers. And having that guidance from you would be very helpful to this committee.

Mr. WILSHUSEN. I'd be happy to talk to your staff to do that, Dr. Coburn.

Senator COBURN. All right. Thank you.

Chairman CARPER. And I'd amend that request to ask that we share that information, as well, with our two compadres on my left, Senator Rockefeller and Senator Thune.

All right, next in order—I think Senator Cowan is next in order, followed by the Senator from New Hampshire, Senator Ayotte.

Senator COWAN. Thank you, Mr. Chairman.

Gentlemen, thank you for your appearance and testimony today.

My first question—actually, my first couple of questions are to you, Mr. Kepler. First, we thank you for coming, and hope you didn't mind me referring to your—you having a platinum system in place.

Just a couple of things, and I wonder if you'd tell me if you agree. It's been said that 85 percent of our nation's critical infrastructure is owned by the private sector. You—and, if that is the case, would you agree that, if the owners of that critical infrastructure fail to harden their systems and we are subject to a cyber attack, that disruption or destruction of those systems could carry catastrophic consequences, not just to the private industry, but to the government sectors that rely upon it? Do you agree with that?

Mr. KEPLER. Yes.

Senator COWAN. And there has been a lot of talk and, I think, a lot of agreement, frankly, that there's a need for more and better

information sharing, and the issues that are, necessarily, surrounding that. Do you think—are you satisfied, from your perspective—and you're someone who looks at these issues, not just for Dow, but I imagine you think about them for your industry, as a whole, or private industry—do you think, if we just have better information sharing and some of those protections, alone, we will have done enough to sort of ensure that, at least at a minimum level, we're doing enough, both in the government and private sector, to thwart cyber threats?

Mr. KEPLER. I think the information sharing is one that lags the most, so the reality is, I think, though—if you think about how you mitigate issue—a risk, in general, it's around applying technology, putting operating disciplines, which you could call "standards," and management systems in place, and then having information sharing about what's going on externally, or competitive intelligence.

I think, over the last 10 years, we've built up a fair amount of capability, and, really, the standards have evolved a lot, and the understanding of how to be responsive around those standards. And the industries that have developed operating discipline around this, I think, is pretty healthy.

I think the key thing that's missing right now is the ability to share tactical information. We're getting attacked, and don't know who from, and we don't have the resources to work on that. I think the threat has changed in the last 5 years, and—to come from outsources with well-resourced resources that need to be addressed.

So, I think the information sharing is a key area. I think the management system around this—because we've got a lot of rules—I think the management system—I think government has to help step up and address.

Senator COWAN. When you talk about the rules—actually, in your testimony, you talked about your concern about overly prescriptive legislation. In my prior job in State government, one of the things I had to do was to sort of oversee the regulatory process. I used to tell the team that the agency heads, before you regulate, hesitate, to think about the cost and the impact on businesses and others.

As you think about the—when you say "overly prescriptive," what, in particular, concerns you that you don't want to see in legislation, or you're concerned that legislation might do?

Mr. KEPLER. Well, I think, when you start looking at these—when you talk to companies like ours, and big companies in structure, you know, you go to some of these sectors, and there are 40,000 or 50,000 companies that you have to deal with, or community structures, if you're in water. And one size does not fit all in that. And you have to be able to assess the risk. So, while you have all the infrastructure, it's not all linked. And so, you have to prioritize this. And, to me, that's the key area that you have to work with the sectors on. If there's any area we need more area is—what enemy are we trying to fight, what problem are we trying to solve, and where are the highest risks in this activity to work on? That's a key area that I—needs to be addressed, or we'll be applying standards and structure to areas that probably have a low priority of risk in that approach.

Senator COWAN. Do you have any viewpoint whether, if we just had a floor, a baseline that everyone—that everyone could look to or try to adhere to, that might better aid us to do—or, to address the concerns?

Mr. KEPLER. Yes. And that's my point on—therefore, you have to have some commitment on—some base floor on the products that you provide people, and how they get configured, and then the responsibility and operating base of how you work on it. So, Dow can bring these resources in, and technologies in, and set them, but a small business that may be linked into this thing, or linked into a supply chain of a critical infrastructure, can't do that. And I think that's where some of this—the industries that supply those products do have to be involved, because the—on the smaller businesses, the same technologies that the consumers use.

Senator COWAN. A question to you, in the first instance, Mr. Kepler, and then, Mr. Wilshusen—and maybe you can answer it, as well. And this—sort of picking up off of the Executive order that the President issued last month—and Mr. Gallagher spoke about, sort of, the collaborative effort between industry and government to come together and work together on some issues—I'm—I wonder if either of you have an opinion about how useful it might be to create a task force composed of government cybersecurity experts, security researchers, and tech vendors to contribute to a database of cyber threats that could be accessed by critical infrastructure industries, in realtime, or issue alerts. When you talk about information sharing, is that something you're thinking of, conceptually?

Mr. KEPLER. Well, conceptually, we have US-CERT, that tries to drive that, for private/public partnership. We have NIAC to look at the policy structures. We have the standard committees to work through.

I think there's a cultural issue on information sharing, is that government does—and I—you know, government doesn't want to share it, and business is reluctant to share it. So, I think the legislation has to go at that cultural aspect and deal with the issues that become the excuses in their liability, on our side, that is important, right?—and their—you know, the IP protection, and those things.

On government, there's a—from an enforcement point of view, you're really nervous about giving up your pursuit of the criminal. And government, by definition, is nervous about trying to manage secrets. So, we have to create an environment where we can share key information on the specific threats. That's, to me, the critical issue here, not the new organization structures. We have a lot of those.

Mr. WILSHUSEN. And I would just add that there is precedence, to some extent, in that there is a database that's maintained by NIST. It's called the "National Vulnerability Database." It's not a database of threats, but it is a database of vulnerabilities that include, for example, software defects, or defective software, and misconfigurations. That database is available to the public to review. And, indeed, many of the tools that are used to scan network devices may draw from that database to look for particular vulnerabilities and misconfigurations in systems.

Senator COWAN. Thank you.

And please forgive my indulgence, Mr. Chairman, for going over my time. Thank you.

Chairman CARPER. No, no, that's fine. Thank you for coming early and staying late——

Senator COWAN. Thank you.

Chairman CARPER.—Senator Cowan.

Senator Ayotte.

STATEMENT OF HON. KELLY AYOTTE,
U.S. SENATOR FROM NEW HAMPSHIRE

Senator AYOTTE. Thank you, Mr. Chairman. I appreciate it.

And I want to thank the witnesses for being here today on such an important issue.

I serve on the Armed Services Committee, as well, and I was inquiring about our top manufacturer in New Hampshire, BAE Systems, just to get a sense of what they've invested in. Just as one company in our state, they've invested over $100 million in their cyber defenses, which, compared to Dow, is probably small, but, I think one thing that they brought to my attention is that they believed, through the interaction they have with the Pentagon, that they have a world class ability to share information. Now, they're a defense contractor, so you can understand why that would be a natural partnership there and that there was a very good collaborative model. While I'm new to this committee, and certainly want to understand the work done by others, one of the worries, I've had, in thinking about this, as I look at the GAO report that was issued, Mr. Wilshusen, and I appreciate the work that you did on this, is the information-sharing difficulties in DHS. And so, we've been talking about some of the concerns we have about DHS's capabilities. Are we trying to use any of the models or patterns from the Pentagon?

And also, it worries me that we're going to have to replicate something that apparently, in the Pentagon, we're doing fairly effectively. And so, how do we take those lessons? And can DHS really get to a point where it is, frankly, as effective as some of the work being done at the Pentagon?

Mr. WILSHUSEN. That's an excellent question. And, indeed, the pilot programs that you're referring to are called the DIB cyber pilot programs. I think they may have another name as well. And DIB being the Defense Industrial Base. Last year, GAO issued a report over those programs and made several recommendations to enhance them. And, as it so happens, we also plan to issue another report that will be coming out soon. The recently issued Executive order has a line in it under—I think it's under the information-sharing section—that asks DHS to look at those programs involving the DIB—the Defense cyber pilot programs—and expand them to the other critical infrastructure sectors. And so, that is one of the activities that is planned.

Senator AYOTTE. Do you think DHS will have the capability to do that? The Pentagon is obviously in a situation where they're dealing with the national security threats, but industries like Dow are dealing with this, a national security threat. So, what's your assessment on DHS's ability? I understand that there's a sort of command to do that in the Executive order, but how can we help

them do that? What's your opinion on what the difficulties will be with that? I don't think any of us want to invest in replicating things that already exist in the government, particularly in the fiscal constraints we find ourselves in.

Mr. WILSHUSEN. No, it's usually a good practice to learn from the efforts of others, to learn both the mistakes, what did not work, as well as what did work, and then apply those lessons as you perform your own. And so, certainly there is a lot of benefit for DHS to do this, and learn from that particular pilot program by DOD.

In terms of DHS's capability to do that, well, I guess we'll actually find out, because I must say that I can't really give you a clear answer on that, because we haven't examined that particular issue. But its success in other programs, previously has been mixed. The department has made some progress in several areas, but, as GAO often reports, more needs to be done.

Senator AYOTTE. So, that worries me, and I hope——

Mr. WILSHUSEN. Yes.

Senator AYOTTE.—that's something we talk about more in this committee, because this is such an important threat to our country that it can't be, "We're just not sure," and, "We don't know how this is going to work out," because, obviously, we need to all work together to make sure we can prevent the threats that are facing the country as well as those facing our businesses and our economic growth.

And I would say, Mr. Kepler, I certainly am reviewing the Executive order, and want to understand it, but, in my prior life, I was an attorney general and thinking about liability protection for the private sector. How does any Executive order really fully get at the type of liability protection that the private sector needs, in light of the fact that, presumably, it's not just liability protection between the government and the industry that's being regulated, but it's also the liability protection to third parties.

Mr. KEPLER. Well, I think that's the challenge. And I think that's one—in my comments, I said that that's one area where I think legislation may be needed to address that.

If you think about major things, like terrorism or whatever, I think there are some vehicles that you can use, with the SAFETY Act, but, if you're trying to look at—you know, I think there are a lot of issues also around intellectual property and legal things that are already defined. When you start looking at issues around espionage and nation state-sponsored commercial espionage, I don't know how—you know, I think that is something you have to think through from a legislative point of view, not an Executive order point of view.

Senator AYOTTE. Well, the prior legislation failed in the Senate so I think all of us want to come to a resolution to find a bipartisan way forward to address these issues, but there certainly seemed to be some areas of difficulty. I know that the liability protection issue is one that Dr. Coburn has already talked about, and of the difficulties there. But, I'm of the view that, since we do a lot of comprehensive work around here, if there are certain areas that we can come to agreement on, then we should move those immediately, and then come back to the other areas that we have to address. So, I'm hoping that this committee, as we work together, will

do that, and continue, as soon as we can get a piece that's important to industry and important to us, moving forward, to having that cooperation, that we will move it.

So, that's my commentary on it. And I'm sure that my time is expired, but I appreciate that both of you are here today, and I look forward to following up with you and learning more about how we can effectively accomplish that.

Chairman CARPER. I thought those were good questions.

Senator AYOTTE. Thank you.

Chairman CARPER. I—we're going to have another round, if it's OK with you, maybe—I'd like to, maybe, do another round. It's not going to take but maybe 15 minutes. Does that work OK with your schedule?

Mr. KEPLER. Sure.

Chairman CARPER. We want to be mindful of your schedules.

Mr. KEPLER. No problem, Senator.

Chairman CARPER. Good. How about another two rounds?

Mr. KEPLER. Whatever you need.

Chairman CARPER. We'll start with one.

One of the things I like to do at the end of the hearing is sometimes to ask witnesses what you've learned—what you've learned by listening to one another, from our questions and some of our statements, what maybe you've learned from the earlier panel. So, just be thinking about what—I mean, what are your take aways from this?

The other thing I would ask you to share with us is what should be our take aways. And when I speak to a group, sometimes I like to tell them what I'm going to tell them, then I tell them, and then I tell them what I've told them. And so, you've had a chance to do at least part of that, and I'm going to ask you, before you leave, to just kind of give that little sum-up at the end, what should be some our key take aways.

For me, one of the key takeaways has been—and I think it was our friend from NIST, Pat—I think he said something like, "When cybersecurity strategy is good business strategy, then we'll know that we've really gotten somewhere." And the—there has been a lot of back-and-forth on information sharing. And Senator Ayotte said she, in her previous life, was attorney general for her state. And I asked some of our staff, "Why don't we do a better job at information sharing from the government side to the private sector?" And someone used this as an example, said, "If you're the FBI, and you're trying to bust a drug ring, and you know—you may let a deal go down, let it happen, just in an effort to move up the food chain and then go after the bigger catches." And I don't know if that's what's going on here, or not, but the—I—one of the messages—for me, one of the take aways is, information flow has to be a two-way street. And so, I take that away.

And on—in terms of the capability of DHS—Dr. Coburn's gone now, but he's—you know, I've been hosting a series of classified briefings, where we have DHS coming in, we have the FBI, we have the National Security Agency coming in. And both he and I have been impressed by the improved capabilities at DHS. This is not your grandfather's Oldsmobile, this is not where they were 10

years ago, 5 years ago. They're—they've gotten some good people, and they've enhanced their capabilities.

I always like to say that the road to improvement is always under construction, so obviously they have more to do. Everything I do, I know I can do better. And certainly that's true for them.

All right. With that having been said, what did you all learn? And, second, what are some good take aways that you would have us to be—just be reinforced with?

Mr. KEPLER. Well, I'd follow up your—just your first point to—or, last point—to comment that I do—when I look at the scope of DHS, and the challenge they have, it's daunting, and I appreciate the work they're doing. And I do agree that the competency of the organization has improved over the years and stuff.

One of the challenges I would say is, we do keep changing the rules a little bit on the number of commissions and structures and groups and things. And so, we're—I'm pleading a little bit for, maybe, stabilization of that and really doing a little bit more oversight on the process, and learning from it.

I think the things I learned—I think we came in feeling that the Executive order had—was in the right spirit of what we were trying to do. We certainly like the concepts of the information sharing. We were very big on standards, to begin with, and we've been that. And I'm very good to see how the Senate, here, is looking at embracing that, and the Executive order has embraced that, and I think they really listened well to the organization. So, I think the spirit of how we want to get there is there.

If you ask me what the two take aways I'd you to leave with, I think is—this risk management, to me, and how we define that, is more important than the standards. I think the standards momentum is there, so we can, you know, put a stamp on it. But, I believe it's used effectively in government and in industry. So, the real issue is, are we really targeting what problem we want to solve? And I think that's really putting definition around "risk management," if you will. So, how do we solve the problems? Who's our real threat? And really make sure form policy around that.

Chairman CARPER. Thanks, Mr. Kepler.

Mr. Wilshusen.

Mr. WILSHUSEN. Yes, I would say one of the take aways would be just to continue providing the oversight and emphasizing follow-through. One of the challenges in the past with the cybersecurity strategies and the different aspects of them has been seeing them all the way through and making sure that there's follow-up, that there are feedback loops. In terms of the agencies, making sure that what they're doing is the right thing to do. The keys for this particular committee is to provide the oversight that it has in the past, and I imagine will continue to do. And certainly, in our role as GAO, it's to continue to help agencies evaluate their progress, and make recommendations, where appropriate.

Chairman CARPER. Senator Thune?

Senator THUNE. Yes, just one last question, if I might, Mr. Chairman, for Mr. Kepler.

And I'm interested in knowing what's the most common cyber attack that your company faces, and how that threat could best be alleviated.

Mr. KEPLER. Yes. If you look at the higher risk ones to—I mean, so you—these numbers sound bizarre, but when you look at the things that used to be a big deal, like viruses—there are still hundreds of thousands of those, and we can protect those pretty well. I think if you tell—you know, what we're challenged with the most is the threats from highly resourced organizations today that are—targeted us and persistent with us. And the concern is, because those are developed, that they end up going down and get learned, and they can migrate down into less sophisticated hands and stuff to work through.

So, I think the fact that we have large organizations—and by—not by my—by my reading, those are some countries and organized criminal organizations—that's a big problem, and it's something that I think government needs to, you know, kind of step in and help business, and actually the country, work on.

Senator THUNE. IP theft?

Mr. KEPLER. You know, I think IP, in general, company to company, it's—the framework of government today manages that. It's this issue now of international and, I think, country-supported IP theft, in doing that, as well as, you know, basically, just general intelligence gathering into companies that had never really happened to the extent we're seeing it now.

Senator THUNE. Thank you all very much. Appreciate it.

Thank you, Mr. Chairman.

Chairman CARPER. You bet.

One last question, if I could, for Mr. Kepler. What is your CEO's name? Andrew——

Mr. KEPLER. Liveris—Andrew Liveris.

Chairman CARPER. Liveris? Well, he came and spoke to a group of us, not long ago. Very impressive. I think he's—may hold a leadership position in the Business Roundtable. Is that true?

Mr. KEPLER. Yes, he does.

Chairman CARPER. And do you know what that is, by chance?

Mr. KEPLER. What his position is? I think he's chairing it, right now, sir.

Chairman CARPER. I think he is, as well. The—we appreciate very much, and need, the continued input from the Business Roundtable. We welcome the input from the Chamber of Commerce—U.S. Chamber of Commerce, and other business groups, as well. But, we're very mindful of the contribution that Business Roundtable can make, and would ask that you pass along our thanks to your CEO and say we'd like to hear more of that, going forward.

Well, it's been a good hearing. And, Senator Thune, whom I affectionately call "Thuney," we are here to the bitter end, but it has not been bitter at all. Not even bittersweet. It has been good. And I—these are—this is a hard issue. Senator Thune and my staff have heard me say this before. This is not an easy issue for me to get my head around. And I—a couple of months ago, I felt like I almost reached the point where I knew enough to be dangerous. And after this hearing today, I know enough to be really dangerous, so—hopefully, really helpful.

And we—it's a shared responsibility, here. It can't be the legislative side to—just on our own. It can't be just the executive branch.

It just can't be the key stakeholders, including the business community. So, it's all of us, together, and—because we have a shared responsibility—and if we do this right, we're going to help our country a whole lot.

And we—Senator Thune and I, our colleagues, Senator Rockefeller and Thune, others who serve on our committees, we want to do this right, and your help—testimony today has certainly helped in that regard.

So, many thanks to you.

And I understand that the hearing record is going to be open for another 14 years.

[Laughter.]

Chairman CARPER. No, not really. Another 14 days, because we're on a short—we're on a short time frame here. Fourteen days for any additional questions or statements from our colleagues. If you get anything, then respond promptly; we'd be most grateful.

Anything else for the record, Senator Thune?

Senator THUNE. No, sir.

Chairman CARPER. With that having been said, it's a wrap. This hearing is adjourned.

Thank you.

[Whereupon, at 5:05 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF THE AMERICAN GAS ASSOCIATION

The American Gas Association (AGA) is pleased to submit this statement for the record for the U.S Senate Committee on Commerce, Science, and Transportation and Committee on Homeland Security and Governmental Affairs joint hearing on *The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting our National and Economic Security* (March 7, 2013). In AGA's view, natural gas is the foundation fuel for a clean and secure energy future providing benefits for the economy, our environment, and our energy security. Alongside the economic and environmental opportunity natural gas offers our country comes great responsibility to protect its distribution pipeline systems from cyber attacks.

Technological advances over the last decade have made natural gas utilities more cost-effective, safer, and better able to serve our customers via web-based programs and tools. Unfortunately, the opportunity cost of a more connected, more efficient industry is that we have become an attractive target for increasingly sophisticated cyber terrorists and cyber thieves. This said, America's investor-owned natural gas utilities are meeting the threat daily via skilled personnel, robust cybersecurity system protections, an industry commitment to security, and a successful ongoing cybersecurity partnership with the Federal Government.

AGA, founded in 1918, represents more than 200 local energy companies that deliver clean natural gas throughout the United States. There are more than 71 million residential, commercial and industrial natural gas customers in the U.S., of which 92 percent—more than 65 million customers—receive their gas from AGA members. AGA is an advocate for local natural gas utility companies and provides a broad range of programs and services for member natural gas pipelines, marketers, gatherers, international gas companies and industry associates. Today, natural gas meets almost one-fourth of the United States' energy needs.

Government-Private Partnerships and Cybersecurity Management: A Process that Works for Natural Gas Utilities

America's natural gas delivery system is the safest, most reliable energy delivery system in the nation. This said, industry operators recognize there are inherent vulnerabilities with employing web-based software and hardware applications for both industrial control systems and business operating systems. Because of this, gas utilities apply myriad cyber standards, guidelines, and related regulations in their cybersecurity portfolios and participate in an array of government-sponsored and industry-sponsored cybersecurity initiatives. However, the most important overall cybersecurity mechanism is the existing cybersecurity partnership between the government intelligence community and industry operators. This two-way information sharing provides for an exchange of vital cybersecurity information within a flexible framework which allows all stakeholders to be proactive and adapt quickly to dynamic cybersecurity risks.

Background: The Homeland Security Act of 2002 provides the basis for Department of Homeland Security (DHS) responsibilities in protecting the Nation's critical infrastructure and key resources (CIKR). The Act assigns DHS the responsibility for developing a comprehensive national plan for securing CIKR. This plan, known as the National Infrastructure Protection Plan (NIPP), identifies 18 critical infrastructure sectors within which natural gas transportation is a subsector of the Energy and Transportation Sectors. The NIPP states that more than 80 percent of the country's energy infrastructure is owned by the private sector, and the Federal Government has a statutory responsibility to safeguard critical infrastructure. For this reason, information-sharing amongst industry operators and the government intelligence community is critical to cyber infrastructure protection.

Process: Natural gas utilities are working with government at every level to detect and mitigate cyber attacks. In particular, the natural gas transportation subsector works specifically with the DHS Industrial Control Systems Cyber Emergency Response Team (ICS–CERT) to reinforce two-way sharing of cybersecurity awareness,

detection, and mitigation programs. This process calls on operators to submit suspicious cyber activity reports to ICS–CERT, while ICS–CERT, in turn, advises operators of noted cyber vulnerabilities, mitigation strategies, and forensic analyses. This open communication has proven over the years to be an effective, uncomplicated mechanism that bolsters the industry's overall cybersecurity posture, while advancing the mission of ICS–CERT. In simple terms, the government intelligence community understands cyber vulnerabilities; natural gas utilities understand their operations; and the two come together in a constructive partnership to protect targeted critical infrastructure.

AGA-Government Cybersecurity Partnerships: AGA works closely with the DHS Transportation Security Administration (TSA), Pipeline Security Division within a government-private industry partnership framework for cybersecurity information sharing. The *Aviation and Transportation Security Act of 2001* gives the TSA Pipeline Security Division regulatory authority over pipeline security for both physical security and cybersecurity. The TSA Pipeline Security Division has over the past decade chosen to partner with pipeline operators in an environment of guidance rather than regulation/compliance. Partnering has benefitted all stakeholders because it allows government and pipeline owner/operators to exchange valuable cybersecurity information typically not shared in a compliance-driven environment.

AGA also strongly encourages industry participation in DHS-led training programs, workshops, and system evaluation programs, available via our partnership with the ICS–CERT and TSA Pipeline Security Division, as well as relevant cybersecurity programs operated by other agencies. Moreover, DHS officials regularly meet with industry groups, such as the AGA board of directors, as well as individual member companies specifically to review and assess ongoing cyberthreats. Bottom line, as cybersecurity threats evolve and related risks to gas industry operations change, our long-standing public-private partnership with DHS allows natural gas utilities to successfully collaborate with the government on overall cybersecurity in a fashion that benefits both parties. The following is a sample list of government-natural gas industry cybersecurity partnerships:

- *DHS Classified and Unclassified Cyber Security Briefings.* Industry operators participate in DHS-sponsored classified and unclassified briefings to receive threat and risk information and analytics. These briefings are in the form of monthly teleconferences and semi-annual face-to-face meetings between the private sector and government intelligence community analysts. The briefings provide information on the state of the subsector in reference to emerging threats, security incidences, and trends. Additionally, AGA is leading the collaborative effort between the government intelligence community and private industry to improve on timely, credible, and actionable information sharing.
- *DHS Control Systems Security Program.* DHS offers various opportunities to enhance industry operator knowledge on control system cybersecurity. Industry operators participate in DHS ICS–CERT training, online forums, recommended practices, advisories, and interactive live assistance focused specifically on control system cybersecurity. Industry operators also receive DHS United States Computer Emergency Readiness Team (US–CERT) monthly activity summaries and secured portal advisory communications, submit incident reports for analysis, and engage in the Industrial Control Systems Joint Working Group for information exchange.
- *Oil & Natural Gas Sector Coordinating Council (ONG SCC) Cyber Security Working Group.* Industry operators participate in this DHS-sponsored forum for effective coordination of oil and natural gas cybersecurity strategies and activities, policy, and communication across the sector to support the Nation's homeland security mission. The ONG SCC provides a venue for operators to mutually plan, implement, and execute sufficient and necessary sector-wide security programs, procedures and processes; exchange information; and assess accomplishments and progress toward protecting the sector's critical infrastructure.
- *TSA Cyber Security CARMA Program.* Sponsored by TSA, this program is intended to develop a nationally-scoped cyber risk management framework to help industry operators identify where internal risk management activities align with industry-wide risk management activities. AGA co-chairs this collaborative effort and facilitates operator participation and contribution.
- *Coordination of Federal Government Risk Assessment Programs.* AGA is proactively coordinating meetings of the Department of Energy, Federal Regulatory Energy Commission, TSA, and ICS–CERT in an effort to encourage all government entities to align their various cybersecurity risk assessment pro-

grams. The objective is to compare/contrast the programs and identify where synergies may be made.

AGA-Industry-Government Cybersecurity Guidelines: Partnership between the private sector and the government is critical to address cybersecurity threats to our Nation's critical infrastructure. As such, AGA and industry operators also collaborate with government partners to produce effective cybersecurity practices and guidelines. Below are a few examples:

- *DHS Transportation Security Administration (TSA), Pipeline Security Guidelines.* Guidelines developed through the collaborative effort of government and pipeline asset owners to be used by natural gas and hazardous liquid transmission pipeline companies, natural gas distribution companies, and liquefied natural gas facility operators as a framework for the protection of critical and non-critical pipeline infrastructure. AGA contributed as subject matter experts, in particular to the cybersecurity chapter.
- *DHS Control Systems Security Program, Cyber Security Evaluation Tool (CSET).* A desktop software tool that guides users through a step-by-step process for assessing the cybersecurity posture of their industrial control system and enterprise information technology networks. AGA participated in the development, testing, and distribution of this material and contributes to continual improvements to this resource.
- *Department of Energy (DOE), Roadmap to Achieve Energy Delivery Systems Cybersecurity.* A strategic framework to improve cybersecurity within the energy sector through a collaborative vision of industry, vendors, academia, and government stakeholders. This vision is supported by goals and time-based milestones for achievement over the next decade. AGA has been a contributor to this resource since its inception in 2006 with its preliminary release as ***DOE, Roadmap to Secure Control Systems in the Energy Sector.***
- *Interstate Natural Gas Association of America (INGAA), Control System Cyber Security Guidelines for the Natural Gas Pipeline Industry.* A set of guidelines designed to assist operators of natural gas pipelines in managing control systems cybersecurity requirements. Aligns with TSA Pipeline Security Guidelines and other guidelines/standards commonly used across the oil and natural gas industries. AGA contributed to the review and comment phase and promotes its availability as a valuable resource to operators and government.
- *AGA and INGAA, Security Practices Guidelines, Natural Gas Industry Transmission and Distribution.* Guidelines that provide an overview of the recommended physical security and cybersecurity practices and procedures for the transmission and distribution segments of the natural gas industry. AGA and the Interstate Natural Gas Association of America lead the initiative to develop this guidance for natural gas pipeline and utility operators.

Non-Standardization of Cybersecurity Practices is Paramount

In the recent past, concerns over increasing cyber attacks—successful or not—on critical infrastructure have led to legislative efforts to create a set of top-down cybersecurity regulations. AGA remains concerned that prescriptive cybersecurity regulations, while well-intentioned, will have little practical impact on cybersecurity and, in fact, will hinder implementation of robust cybersecurity programs. First and foremost, prescriptive cybersecurity regulations would fundamentally transform the productive cybersecurity relationship natural gas utilities have with the TSA Pipeline Security Division from a successful partnership to a more standard regulator-regulated mode, forcing companies to focus more resources on compliance activities than on cybersecurity itself. Also, from a practical perspective, it is unlikely that any set of cybersecurity regulations will be dynamic enough to help companies fight constantly changing and increasingly sophisticated threats.

Across the natural gas industry, cybersecurity effectiveness is maximized through the diversity of individual company cybersecurity approaches, *e.g.,* Defense in Depth strategies and customized detection and mitigation systems appropriate for individual company networks. Furthermore, because gas utility control system operations vary amongst operators, companies adhere to cyber standards, guidelines and related regulations most relevant to their specific network functions and vulnerabilities. Companies also turn lessons learned from government-private industry cybersecurity information sharing partnerships into actions designed to protect their specific systems. In sum, as cybersecurity risks and threats change, so do vulnerabilities. Ongoing implementation of new and diverse cybersecurity tools and procedures, based on unique individual company requirements, helps companies

adapt to a dynamic cyberthreat environment and bolsters the overall gas utility industry cybersecurity posture.

The Cybersecurity Executive Order Considered

The Administration's Executive Order (EO), *Improving Critical Infrastructure Cybersecurity,* is a data collection exercise, standards setting program, and outline for future legislative and regulatory action. In sum, the EO directs the government to: (1) identify all critical infrastructure entities, (2) prepare "voluntary" cybersecurity standards for identified critical infrastructure, (3) develop incentives designed to entice entities to adopt the cybersecurity standards, and (4) tasks agencies with existing cybersecurity authorities to determine whether their current regulations are sufficient or if new, more prescriptive, cybersecurity regulation is necessary.

Clearly, Congress will be a not-so-silent partner in implementing this EO, particularly if agencies with cybersecurity responsibilities, having found current programs inadequate, lack the authority necessary to further regulate cybersecurity requirements in their sector. In addition, while the EO does seek to strengthen the public-private cybersecurity information sharing partnership, liability and information security protections necessary for critical infrastructure owners and operators to fully participate will require new statutory authority.

Overall, the EO is simply the beginning of a long march to improve national cybersecurity. AGA is hopeful, and will work to ensure, that throughout this policy process gas utility industry cybersecurity concerns will be addressed. To that end, below are a few of our specific concerns with the EO.

Identifying Critical Infrastructure. The executive order confines itself largely to "critical infrastructure", a categorization that undoubtedly will include natural gas utilities. Critical infrastructure is defined in Section 2 of the EO as *"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."* Note that the EO does not define many terms included in the definition ("debilitating impact", "economic uncertainty", etc.), potentially opening an ongoing debate over what systems may be considered critical or not critical. In addition, AGA strongly suggests that the identification process include the active and informed participation of critical infrastructure owner/operators from the start rather than after the assignment of "critical" has been determined by the government. By doing this, the government avoids placing the owner/operator in a defensive position with the burden to demonstrate non-criticality. Further, any list must be secured with appropriate information protection mechanisms.

Cybersecurity Information Sharing Program. Section 4 of the EO creates a cybersecurity information sharing program, directing DHS, the Department of Justice, and the Office of the Director of National Intelligence to set up cyber threat information sharing processes with targeted private sector entities. Without question, improved information sharing can and will benefit critical infrastructure cybersecurity. However, for industry to fully engage in an information sharing program, information protection mechanisms (safe harbors) and liability protections must be afforded to owners/operators who participate in the program. Without such protections, companies may be unwilling to participate because of the possibility of information leaks as well as due to competitive concerns and legal liability pressures.

NIST "Cybersecurity Framework". Section 7 of the EO directs the National Institutes of Standards and Technology (NIST) to develop, via an open review process, a "Cybersecurity Framework" designed to improve critical infrastructure cybersecurity. The Framework will utilize risk and performance based standards/best practices; technology neutral applications; voluntary consensus standards and industry best practices; and cross-sector security standards applicable to all critical infrastructure. Ultimately, NIST's goal is to create a framework that is "prioritized, flexible, repeatable, performance-based, and cost-effective" to help critical infrastructure owner/operators manage cyber risk. Good intentions notwithstanding, questions remain, including:

- Given the complexity of the subject, will NIST be able to meet notice and comment timelines?
- Will the final Framework be flexible enough to address every critical infrastructure sector?
- How much influence will critical infrastructure sectors have in developing the Framework?
- Will the Framework morph into mandatory standards?

Industry Adoption of Cybersecurity Framework. Section 8 of the EO directs DHS to create a "voluntary" program to spur critical infrastructure entities to adopt the NIST Framework. Specifically, DHS will work with other agencies to review the Framework and develop implementation guidance to address sector-specific operating environments. More importantly, DHS will work with the Departments of Commerce and Treasury to report on existing incentives that might spur industry participation in the voluntary program as well as any additional incentives (*i.e.,* liability protections) that would require new statutory authority. Sector agencies will also report annually on which critical infrastructure owner/operators participate in the program. Overall, just how "voluntary" this program ends up becoming is an open question. As AGA and other critical infrastructure industries have argued, voluntary government programs often morph into de facto mandatory compliance programs because companies feel compelled to participate rather than risk opening themselves up to litigation for not engaging in a program that has the imprimatur of the Federal Government.

Agency Adoption of NIST Cybersecurity Framework. Section 10 of the EO notes that once the NIST Framework has been preliminarily drafted agencies with cybersecurity regulatory responsibilities will review their existing authorities to determine whether they are sufficient given the cyberthreat landscape, and whether they can implement the NIST Framework via regulation. If agencies determine that their current cybersecurity regulatory requirements are insufficient then they shall propose new "actions" to mitigate cyber risks. This section clearly pushes sector agencies to create new cybersecurity regulations. These new requirements would, at a minimum, be based upon the NIST Cybersecurity Framework; however, there is plenty of suggestion in Section 10 that agencies move beyond the framework, or seek the authority to do so. We are hopeful this will not lead to regulation for regulations sake. For example, despite having the statutory authority necessary, TSA Pipeline Security Division has chosen not to issue cybersecurity regulations for natural gas utilities in large part because of the successful security partnership we have collectively developed.

The Case for Cybersecurity Legislation

Despite our concerns about prescriptive cybersecurity standards, AGA does believe that there is a role for cybersecurity legislation, particularly as it relates to improving public-private cybersecurity information sharing and related liability protections.

Information Sharing. To help counter cyber attacks and protect networks against future incursions, critical infrastructure needs government to help them identify, block and/or eliminate cyberthreats as rapidly and reliably as possible. From a functional perspective, this will require expediting security clearances for critical infrastructure personnel as well as streamlining the process by which actionable threat intelligence is shared with private industry. Harnessing the cybersecurity capabilities of the government intelligence community on behalf of private sector networks will go a long way towards overall network security. The recently introduced H.R. 624, *The Cyber Intelligence Sharing and Protection Act* (CISPA) begins to flesh out this process by establishing a cybersecurity partnership between critical infrastructure and the intelligence community. However, there is certainly a role the Department of Homeland Security can play, as a sector specific agency, in distributing cyberthreat information, interpreting potential threat impacts, and working with critical infrastructure entities to keep their networks safe. This would particularly be the case for those industries, like natural gas utilities, that already have a cybersecurity partnership with TSA.

Liability Protection, SAFETY Act. Another avenue for legislation surrounds offering liability protection for companies with robust cybersecurity programs—standards, products, processes, etc. The Administration's recent executive order (EO) on cybersecurity underscores this need. The EO directs sector agencies, the intelligence and law enforcement community to establish a cybersecurity information sharing partnership; tasks the National Institute of Standards and Technology with establishing a quasi-regulatory set of cybersecurity standards (a "cybersecurity framework"); and orders DHS to incentivize critical infrastructure to adhere to the NIST standards. What the EO cannot do is provide liability protections for critical infrastructure entities that make the effort to participate in a public-private cybersecurity program, regardless of whether it is created via EO or some future law.

AGA supports employing the *SAFETY Act* as an appropriate avenue for providing companies that participate in a government-private industry cybersecurity partnership with liability coverage from the impacts of cyberterrorism. *SAFETY Act* applicability in this area seems plain:

- *The SAFETY Act* exists in current law, and a related office at DHS has been reviewing and approving applications for liability coverage in the event of an act of terrorism or cyber attack for over a decade. This office utilizes an existing review and approval process which would allow for immediate granting of liability protections from cyber attacks.
- Because the *SAFETY Act* can apply to a variety of areas ranging from cybersecurity standards (cyber best practices, etc.), to procurement practices and related equipment (SCADA, software, firewalls, etc.) companies can layer their liability protection.
- We are aware of no other existing statute that offers similar liability protections. Moreover, we do not see the need to write new law to address liability protections from cyber incidents when the *SAFETY Act* is already applicable.

This said, there are some areas where we believe the *SAFETY Act* could be a little stronger as it applies to cyber matters. First, and foremost, the statute could be expanded to make specific reference to liability protections from "cyber" events (cyber attacks, cyber terrorism, etc.) and more specific reference to coverage for cybersecurity equipment, policies, information sharing programs, and procedures. While there is coverage under the Act currently for cyber attacks, specifically identifying "cyber attacks" as a trigger for liability protections would strengthen the overall concept.

The Natural Gas Utility Cybersecurity Posture

AGA's policy priorities for cybersecurity include preserving our current cybersecurity partnership with the Transportation Security Administration, Pipeline Security Division, enhancing government-private industry cybersecurity information sharing, opposing burdensome or counterproductive cybersecurity regulation, and supporting robust liability protections for entities that are serious about protecting their networks. If ultimately achieved, these items will only bolster an already solid industry cybersecurity commitment.

America's natural gas utilities are cognizant of enduring cyber threats and the continued need for vigilance through cybersecurity protection, detection, and mitigation mechanisms. Industry operators apply numerous cyber standards, guidelines, and related regulations in their cybersecurity portfolios and participate in a variety of government-sponsored cybersecurity initiatives. There is no single solution for absolute system protection. However, through a combination of cybersecurity processes and timely and credible information-sharing amongst the government intelligence community and industry operators, America's natural gas delivery system remains protected, safe and reliable, and will remain so well into the future.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO HON. JANET NAPOLITANO

Question. The Executive Order requires agencies to incorporate privacy and civil liberties safeguards into their activities. Yet the fact that a Federal Government-private sector cyber information-sharing program must be streamlined and rapid in order to be effective poses unique privacy challenges. Can you provide concrete examples of how DHS and other agencies will implement these safeguards even as they increase information sharing with the private sector? The Fair Information Practice Principles of an individual's access to collected data and the preservation of the integrity of that data would seem to be particularly difficult to ensure in the pursuit of sophisticated cyber threats. How will the need for a better flow of information, sometimes including classified information, be balanced with these principles? Do you believe that current law adequately protects privacy rights in cyberspace, particularly if information-sharing between the government and private sector is increased? Do you believe that cyber legislation focusing solely on the issue of information sharing that has been previously proposed in Congress, such as the Cyber Information Sharing and Protection Act (CISPA), adequately address these privacy and civil liberties concerns?

Answer. In recognition of the privacy and civil liberties concerns associated with the efforts called for in Executive Order (EO) 13636, the Administration directed Departments and Agencies to assess activities required by EO 13636 for potential privacy and civil liberties risks. In developing this and other documents, the Administration sought input from stakeholders of all viewpoints in industry, government, and the advocacy community. Their input has been vital in crafting an order that incorporates the best ideas and lessons learned from public and private sector efforts while ensuring that our information sharing incorporates rigorous protections for individual privacy, confidentiality, and civil liberties. Indeed, as we perform all

of our cyber-related work, we are mindful of the need to protect privacy, and civil liberties. The Department has implemented strong privacy and civil rights and civil liberties standards into all its cybersecurity programs and initiatives from the outset.

Rather than simply attempting to balance information sharing with privacy concerns, Departments and Agencies will use the Fair Information Practice Principles (FIPPs) as an analytical framework to assess privacy risks and integrate privacy protections into their cybersecurity programs. The FIPPs help agencies recognize the importance of data minimization, that is, that agencies should only collect information that is relevant and necessary to accomplish agency missions. Not only does this ensure privacy, but it also facilitates more effective protection of critical cybersecurity infrastructure. A concrete example of how DHS implements the FIPPs is by conducting Privacy Impact Assessments (PIAs) on the Department's cyber systems and programs. DHS published the Enhanced Cybersecurity Services (ECS) PIA in January of this year and will continue to update or conduct PIAs on cyber operations on an ongoing basis. The ECS PIA describes the operational processes and privacy and security oversight required to share unclassified and classified cyber threat indicators with companies that provide internet, network and communications services to enable those companies to enhance their service to protect U.S. Critical Infrastructure entities.

In addition, the Federal Government will ensure that privacy and civil liberties safeguards are incorporated into cyber activities through the work of the recently formed Assessments Working Group (WG) under the Integrated Task Force (ITF), which leads the Administration's implementation efforts of the requirements laid out in the EO and Presidential Policy Directive-21 (PPD–21). The WG is an interagency body whose participants represent Senior Agency Officials for Privacy and Civil Liberties. The WG is responsible for providing support to Departments and Agencies as they conduct the privacy and civil liberties assessments required by Section 5 of EO 13636. The WG will serve as a forum for sharing approaches to conducting these assessments. Separately, the DHS Privacy Office and Office for Civil Rights and Civil Liberties (CRCL) will conduct assessments of DHS activities undertaken pursuant to the EO, and will compile other Departments' and Agencies' assessments for inclusion in an annual report. In compiling the report, the Privacy Office and Office for Civil Rights and Civil Liberties (CRCL) will consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget, consistent with the requirements set forth in EO 13636.

In addition, the DHS Privacy Office and Office for Civil Rights and Civil Liberties has hosted a series of five meetings for privacy and civil liberties advocates that began in April 2013 to provide additional transparency into the operation of the ITF Working Groups.

It is important to note that the Executive order does not grant new regulatory or other authority to increase voluntary cooperation with the private sector or to establish additional incentives for participation in the Voluntary Critical Infrastructure Cybersecurity Program established in the EO. New approaches to cybersecurity are urgently needed, and we are committed to working with Congress for passage of a comprehensive suite of legislation.

The Administration's legislative priorities for the 113th Congress build upon the President's 2011 Cybersecurity Legislative Proposal and take into account two years of public and congressional discourse about how best to improve the Nation's cybersecurity. Congress should enact legislation to incorporate privacy and civil liberties safeguards into all aspects of cybersecurity; strengthen our critical infrastructure's cybersecurity by further increasing responsible information sharing and promoting the establishment and adoption of standards for critical infrastructure; giving law enforcement additional tools to fight crime in the digital age; and creating a National Data Breach Reporting requirement.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KELLY AYOTTE TO HON. JANET NAPOLITANO

Question 1. The issue of cyber security is far too important not to find common ground and move forward with legislation that would make us safer today. Some like to blame different associations or trade groups for the inability to get legislation through both bodies of Congress, but I would argue that Republicans and Democrats agree on a vast majority of the issues being debated. Why can't we pass what we all agree on, such as information sharing and then roll up our sleeves and see if we can find consensus on the issues where there may not be as much common ground? Too much is at stake to have an all-or-nothing mentality.

Answer. Both sides of the aisle are united in their recognition that cybersecurity must be strengthened. While the Administration has taken significant steps to protect against evolving cyber threats, we must acknowledge that the current threat outpaces current authorities. In the current landscape, DHS must execute its cybersecurity mission under an amalgam of existing statutory and executive authorities that have failed to keep up with the responsibilities. Cybersecurity activities have made clear that certain laws that govern cybersecurity activities must be updated.

In February 2013, President Obama issued Executive Order 13636 on Improving Critical Infrastructure Cybersecurity as well as Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, which will strengthen the security and resilience of critical infrastructure through an updated and overarching national framework that acknowledges the increased role of cybersecurity in securing physical assets. These directives create a foundation for legislative action by implementing concepts set forth in the President's 2009 Cyberspace Policy Review, and policies drawn from the recommendations of the House Republican Cybersecurity Task Force and the bipartisan Commission on Cybersecurity for the 44th Presidency.

It is important to note that the Executive order directs Federal agencies to work within current authorities and increase voluntary cooperation with the private sector to provide better protection for computer systems critical to our national and economic security. It does not grant new regulatory authority or establish additional incentives for participation in a voluntary program. New approaches to cybersecurity are urgently needed, and we are committed to working with Congress for passage of a comprehensive suite of legislation.

The Administration's legislative priorities for the 113th Congress build upon the President's 2011 Cybersecurity Legislative Proposal and take into account two years of public and congressional discourse about how best to improve the Nation's cybersecurity. Congress should enact legislation to incorporate privacy, confidentiality, and civil liberties safeguards into all aspects of cybersecurity; strengthen our critical infrastructure's cybersecurity by further increasing information sharing and promoting the establishment and adoption of standards for critical infrastructure; give law enforcement additional tools to fight crime in the digital age; and create a National Data Breach Reporting requirement.

Question 2. If the Federal Government deems a business as covered critical infrastructure, but that business disputes whether or not it should be covered, what is the appeal process? Do businesses have any recourse or is DHS judge and jury in this instance?

Answer. Under Executive Order (EO) 13636, private sector participation in cybersecurity matters with the Department of Homeland Security (DHS) is carried out on a voluntary basis and supports more efficient sharing of cyber threat information. The EO directs the National Institute of Standards and Technology to develop a Cybersecurity Framework to identify cybersecurity practices among critical infrastructure sectors and directs DHS to develop a Voluntary Program to encourage adoption of the Framework. While the intent of the EO is to offer additional cybersecurity capabilities to assist owners and operators of critical infrastructure, with the expectation that accepting this assistance will be in the firms' best interest, EO 13636 creates no new legal obligation for businesses to adopt any cybersecurity measures.

Because the vast majority of U.S. critical infrastructure is owned and operated by private companies, reducing the risk to these vital systems requires a strong partnership between government and industry. To implement EO 13636, DHS engaged in a consultative process with public and private sector partners to identify critical infrastructure that if impacted by a cybersecurity incident could reasonably cause catastrophic impacts to our national security, economic security, public health and safety. Specifically, EO 13636 requires consultation with the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector Specific Agencies; other relevant agencies; independent regulatory agencies; state, local, territorial, and tribal governments; universities; and outside experts.

DHS will confidentially notify owners and operators of critical infrastructure identified under this process and ensure identified owners and operators are provided the basis for the determination. The Department is also required to establish an administrative appeals process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of their identification as "critical infrastructure of greatest risk."

Question 3. Earlier this month in a Senate Armed Services hearing, Gen. James Mattis, the Commander of U.S. Central Command testified that with the increasing role of our adversaries in cyberspace, it only adds more urgency to expand our presence, capabilities and authorities to maintain an advantage in cyberspace. Threat networks, including those posed by Iran and China, are adjusting opportunistically. What role do you envision DHS playing to destabilize cyber activities that lead to, among other things, transfer of illicit arms, espionage and aid transferred to support malign actors seeking to undermine our security? What forums exist and what forums are you considering using to put more urgency and high level attention into the DHS–CYBERCOM cyber security dialogue?

Answer. The United States confronts a dangerous combination of known and unknown vulnerabilities in cyberspace and strong and rapidly expanding adversary capabilities. Successful response to dynamic cyber threats requires a whole of government approach leveraging homeland security, law enforcement, and military authorities and capabilities, which respectively promote domestic preparedness, criminal deterrence and investigation, and national defense. While each agency operates within the parameters of its authorities, the U.S. Government's response to cyber incidents of consequence is coordinated among the Department of Homeland Security (DHS), Department of Justice (DOJ), and the Department of Defense (DOD) such that "a call to one is a call to all."

DHS is responsible for coordinating the Federal Government response to significant cyber or physical incidents affecting critical infrastructure, consistent with statutory authorities. The Department is the largest law enforcement agency in the Federal Government, with personnel stationed in every state and in more than 75 countries around the world. To combat cyber crime, DHS relies upon the skills and resources of the United States Secret Service (USSS), U.S. Immigration and Customs Enforcement (ICE), U.S. Coast Guard, and U.S. Customs and Border Protection (CBP) and works in cooperation with partner organizations, including international partners, to investigate and prosecute cyber criminals and works in cooperation with partner organizations, including international partners, to investigate and prosecute cyber criminals. (Pursuant to section 1030 of the Title 18 of the United States Code, the Federal Bureau of Investigation has primary authority to investigate cyber crimes with a national security, counterintelligence, or espionage nexus.)

Additionally, there are several key ways in which DHS leverages the capabilities of the DOD. DHS is able to draw upon specific classified cyber threat intelligence that can be utilized in enhancing the protection of Federal networks and private critical infrastructure networks under cooperative partnerships. The DHS–DOD relationship also includes a Memorandum of Agreement for exchanges of personnel as well as shared technical expertise. I meet regularly with Director Mueller and General Alexander to coordinate and align operational strategies.

DHS has administrative security authorities that allow it to defend government networks, to share and receive threat information with private, State, local and tribal entities, and to coordinate with our intelligence community and law enforcement agency partners and to leverage government cybersecurity expertise and render technical assistance when needed.

Synchronization among DHS, DOJ, and DOD ensures that all of government's capabilities are brought to bear against cyber threats and enhances government's ability to share timely and actionable cybersecurity information with a variety of partners, especially the private sector.

Question 4. A new report from the Pentagon's Defense Science Board on cyber threats has raised some grave concerns. Among its findings, our cyber capabilities at the Pentagon are "fragmented" and the Defense Department is not prepared to defend against this threat." It goes on to say that the Pentagon cannot be confident that its military computer systems are not compromised because some use components made in countries with high-end cyber-capabilities such as China and Russia. Do you share the concerns of this Pentagon Report?

Answer. The Department of Homeland Security (DHS) has reviewed the report and values this contribution provided by the Defense Science Board. We agree that the cyber threat is serious, that public and private networks in all countries are built on inherently insecure architectures, and that the United States should lead the way by taking positive action to increase the security and confidence in the information technology systems we depend on. We have reviewed the recommendations and findings of the report and are working to apply lessons learned to our own mission to protect Federal Civilian Executive branch networks. Additionally, DHS, along with interagency partners, is aggressively implementing the National Strategy for Global Supply Chain Security of January 2012, which seeks to protect the welfare and interests of the American people and secure our Nation's economic pros-

perity by promoting the secure movement of goods and fostering a resilient supply chain.

Question 5. Do you feel countries like China and Russia are ahead of the U.S. on the technology scale when it comes to cyber? How confident are you that the computer systems used by your agency are not vulnerable since so many are made overseas?

Answer. We would be happy to provide a threat briefing in a classified setting.

Question 6. What is DHS's working relationship and division of labor between Cyber Command and DHS?

Answer. Ensuring the Nation's cybersecurity is a shared responsibility. Successful response to dynamic cyber threats requires a whole of government approach leveraging homeland security, law enforcement, and military authorities and capabilities, which respectively promote domestic preparedness, criminal deterrence and investigation, and national defense. While each agency operates within the parameters of its authorities, the U.S. Government's response to cyber incidents of consequence is coordinated among DHS, the Department of Justice (DOJ), and Department of Defense (DOD) such that "a call to one is a call to all."

As with all threats to the United States, our allies, and our interests in other domains, the DOD has the mission to defend the Nation against foreign attacks. Its national security mission demands that it defend, deter, and take decisive action in cyberspace to defend our national interests. DHS is responsible for securing unclassified Federal civilian government networks and working with owners and operators of critical infrastructure to secure their networks through risk assessment, mitigation, and incident response capabilities.

While each department has its own separate role, there is a high level of cooperation on cybersecurity activities including the U.S. Cyber Command, DHS/NCCIC, and NSA's Threat Operations Center. Collaboration between these designated 'cyber centers' has been maturing since the approval of HSPD–23/NSPD–54 in 2007. To further cooperation between DOD and DHS, a memorandum of agreement was signed in October 2010 that formalized coordination processes, embeds DOD cybersecurity analysts within DHS and puts DHS leaders and analysts inside the National Security Agency to foster operational coordination. (This agreement was codified in the *National Defense Authorization Act for Fiscal Year 2012,* P.L. 112–81, Sec. 1090.) Additionally, I meet regularly with General Alexander to coordinate and align operational strategies.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN COATS TO HON. JANET NAPOLITANO

Question 1. The President's Executive Order focuses on threats to the Nation's critical infrastructure, and yet numerous open source reports indicate state sponsored industrial and economic espionage against American businesses is an equal if not greater threat to America's national and economic security. For example, last year General Keith Alexander spoke at an AEI event and called industrial cyberespionage and intellectual property theft "the greatest transfer of wealth in our Nation's history." He estimated the costs to the American economy to be $388 billion, and a 2011 report from the Office of National Counter-Intelligence Executive estimated the costs to the American economy to be in the $400 billion range, with Chinese actors as the world's most active perpetrators of industrial cyberespionage. As you also know, the cybersecurity firm Mandiant released a report this year documenting the problem of Chinese economic/industrial espionage, specifically looking at the "advanced persistent threat" (APT) from one of the Chinese People's Liberation Army (PLA) cyberattack units. How would you compare the threat to our economic interests to the threat to critical infrastructure?

Answer. The Department of Homeland Security (DHS) continues to be concerned about the effects of cyber-enabled theft of intellectual property, trade secrets and commercial data, and works daily with interagency partners and the private sector to address the threat. Additionally, while the consequences of wide-scale intellectual property theft may be different than those from a destructive or disruptive cyber attack to critical infrastructure, techniques that adversaries may use to steal sensitive business information also expose vulnerabilities that could be used to destroy or disrupt critical systems and services. Both are very real threats of potentially high consequence, and we take them very seriously. In fact the things we must do to address them both are quite similar.

To combat cyber crime, DHS relies upon the skills and resources of the United States Secret Service (USSS), U.S. Immigration and Customs Enforcement (ICE), U.S. Coast Guard (USCG), and U.S. Customs and Border Protection (CBP) and

works in cooperation with partner organizations to investigate cyber criminals. Since 2009, DHS has prevented $10 billion in potential losses through cyber crime investigations and arrested more than 5,000 individuals for their participation in cyber crime activities. The Department leverages the 31 USSS Electronic Crimes Task Forces (ECTF), which combine the resources of academia, the private sector, and local, state and Federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructure. The Department is also a partner in the National Cyber Investigative Joint Task Force, which serves as the national focal point for U.S. Government coordination, integration, and sharing of information relating to all domestic national security cyber investigations sharing across the interagency. To further these efforts, the Administration issued its Strategy on Mitigating the Theft of U.S. Trade Secrets in February of this year. DHS will act vigorously to support the Strategy's efforts to combat the theft of U.S. trade secrets—especially in cases where trade secrets are targeted through illicit cyber activity by criminal hackers.

In addition, DHS works with its interagency partners to distribute relevant technical threat data to industry partners enabling them to take action to prevent and mitigate potential network intrusions and cyber-enabled theft. The DHS Enhanced Cybersecurity Services (ECS) program is one of many efforts to increase this sharing of technical threat data. Under ECS, DHS provides classified and sensitive threat information to qualified cybersecurity providers, who then utilize this information to offer enhanced cybersecurity services to many businesses that qualify as critical infrastructure entities. However, just as with addressing threats to physical critical infrastructure, we must have two-way and real-time information exchange among government agencies, network owners and operators, and others in order to more fully understand what malicious cyber activity is occurring and how to best address it. We look forward to working with Congress to find ways to further increase this critical information sharing relationship and incentivize the adoption of cybersecurity best practices by critical infrastructure partners.

Question 2. A GAO report released last month found that cybersecurity incidents at Federal agencies were on the rise. And while there is an uptick in these incidents, challenges remain in how DHS is carrying out responsibilities in sharing information among Federal agencies and key private sector entities such as critical infrastructure owners. The GAO report also found that DHS is not "developing a timely analysis and warning capability," citing that the Inspector General at DHS recommended that DHS establish a "consolidated, multiple-classification-level portal to share incident response related information" which DHS says will not be ready until 2018. The report also found that Federal Information Security Management Act compliance is inadequate, with only 8 of 22 agencies being in compliance with FISMA standards in 2011 (down from 13 out of 24 agencies in 2010) and that 9 agencies "had not fully developed required policies for monitoring security on a continuous basis." Since, according to GAO and various agency Inspectors General, the Federal Government has demonstrated it is unable to meet its requirements under FISMA, what confidences should we have that it is prepared to regulate and oversee private sector operations of critical infrastructure?

Answer. Significant progress has been made in improving information sharing among the Department of Homeland Security's (DHS) Office of Cybersecurity and Communication, Federal agencies, and other partners and constituents. DHS provided documentation of its improved public-private cybersecurity information sharing activities to Government Accountability Office (GAO) in August 2011, promptly answered subsequent questions, and are awaiting GAO's closure of the associated recommendations under GAO's report on *Key Private and Public Cyber Expectations Need to be Consistently Addressed.* Additionally, GAO closed all ten recommendations under the Cyber Analysis and Warning report.

Protecting critical infrastructure against growing and evolving cyber threats requires a layered approach. DHS is committed to ensuring cyberspace is supported by a secure and resilient infrastructure that enables open communication, innovation, and prosperity while protecting privacy, confidentiality, and civil rights and civil liberties. The Department has operational responsibilities for securing unclassified Federal civilian government networks and working with owners and operators of critical infrastructure to secure their networks through cyber threat analysis, risk assessment, mitigation, and incident response capabilities. DHS is also responsible for coordinating the national response to significant cyber incidents and for creating and maintaining a common operational picture for cyberspace across the government.

In September 2012, DHS finalized the Strategic National Risk Assessment (SNSRA) Report for Communications in coordination with public and private sector partners and is currently working with industry to develop plans for mitigating

risks identified in the SNSRA, which will determine the path forward in developing outcome-oriented performance measures for cyber protection activities related to the Nation's core and access communications networks. In addition, in February 2013, the President issued Executive Order 13636 on Improving Critical Infrastructure Cybersecurity as well as Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, which will strengthen the security and resilience of critical infrastructure through an updated and overarching national framework that acknowledges the increased role of cybersecurity in securing physical assets. Executive Order 13636 expands the voluntary DHS Enhanced Cybersecurity Service program, which promotes cyber threat information sharing between government and the private sector. This engagement helps critical infrastructure entities protect themselves against cyber threats to the systems upon which so many Americans rely.

DHS actively collaborates with public and private sector partners every day to improve the security and resilience of critical infrastructure while responding to and mitigating the impacts of attempted disruptions to the Nation's critical cyber and communications networks and to reduce adverse impacts on critical network systems. Such partnerships, combined with existing DHS critical infrastructure cybersecurity programs, assure that DHS will have the relationships and expertise to implement an oversight and compliance regime. Examples of existing programs include the Cyber Information Sharing, and Collaboration Program, which enables regular and trusted sharing of actionable cybersecurity threat indicators that those owners and operators can immediately use for computer network defense activities. Additionally, DHS has long served as the Sector Specific Agency for both the Information Technology and Communications sectors. This trusted partnership has enabled further collaborative initiatives such as the Information Technology Sector Risk Assessment, the Cybersecurity Evaluation Program, which conducts voluntary cybersecurity assessments across all critical infrastructure sectors, and the Critical Infrastructure-Cyber Security program that leads efforts with public and private sector partners to promote an assured and resilient U.S. cyber infrastructure.

DHS also conducts daily operational, information sharing, incident response, and technical assistance through the National Cybersecurity and Communications Integration Center (NCCIC) and its components. Every day, partners from private sector critical infrastructures, Information Sharing and Analysis Centers, Federal cybersecurity centers, and international governments collaborate on cybersecurity response and information sharing through the NCCIC. DHS directly supports Federal civilian departments and agencies in developing capabilities that will improve their cybersecurity posture in accordance with the Federal Information Security Management Act (FISMA). To protect Federal civilian agency networks, our National Protection and Programs Directorate (NPPD) is deploying technology to detect and block intrusions through the National Cybersecurity Protection System and its EINSTEIN protective capabilities, while providing guidance on what agencies need to do to protect themselves and measuring implementation of those efforts. Under current authorities though, DHS can only monitor, recommend security posture improvements, and report on Federal agencies' compliance with FISMA. As the GAO report notes, the current law should be updated to give DHS the statutory authority it needs to fulfill the responsibilities it has been given.

NPPD is also developing a Continuous Monitoring as a Service (CMaaS) capability. Through an automated and continuously updated analytical process, the deployed .gov agency sensors will provide data to a centralized dashboard. Cyber risk related data will be updated and displayed daily for management and technical staff review that will provide insight into network vulnerabilities to more readily prioritize for the purposes of ongoing mitigation. When combined, the overall results from Departments and Agencies will contribute toward improving the agency-specific, as well as the Federal Executive Branch overall cyber risk posture. This capability will support compliance with Administration policy, be consistent with guidelines set forth by the National Institute of Standards and Technology (NIST), and enable Federal agencies to move from compliance-driven risk management to data-driven risk management. These activities will provide organizations with information necessary to support risk response decisions, security status information, and ongoing insight into effectiveness of security controls.

DHS partnered with the General Services Administration (GSA) to award a blanket purchase agreement (BPA) under which CDM tools and services can be provided to government entities. The BPA, with an anticipated $6-billion ceiling for the five years (one-year contract with four one-year options), is open to all Federal civilian and defense organizations, as well as state and local government entities. The significant size of the CDM contract was designed to compatibly support not only Federal civilian network protection assigned to DHS, but the large body of cybersecurity

requirements for any Federal custom and cloud application over the life of the contract which are funded separately by each department and agency.

Congress provided funding in the DHS Appropriations Act, 2013 (P.L. 113–6) to implement Continuous Diagnostics and Mitigation (CDM) across civilian Executive Branch agencies in order increase our ability to identify and track threats, find vulnerabilities, mitigate the worst issues first and report on progress in doing so. CDM and FISMA legislative reforms that provide clear statutory authorities for carrying out the DHS mission would have the following benefits:

- Improved security posture leading to improved regulatory compliance
- Standard security configurations across all Federal Executive Branch civilian department and agency critical network infrastructure
- Improved communication and collaboration methods across diverse stakeholder groups
- Improved situational awareness creates synergy amongst the Federal cybersecurity workforce and improves communication and information sharing within the Federal enterprise
- Increased efficiency and security posture through collaboration and streamlining

In addition, DHS works with critical infrastructure stakeholders in the private sector through the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT). These relationships are maintained by ICS–CERT through cybersecurity incident analysis and onsite assistance, training opportunities in control systems security development, and the Industrial Control Systems Joint Working Group (ICSJWG).

Question 3. The Executive Order focuses solely on government-to-private-sector information sharing. Many believe, and I agree, that better private-to-government and private-to-private information sharing protocols need to be implemented, and I question how we can get there without better liability protections. What is your plan to encourage better private-to-government and private-to-private information sharing? How will the Framework incentivize private sector partnership without these carrots? Is it possible that private companies may withhold participation in the Framework until such incentives are provided through legislation?

Answer. While Executive Order (EO) 13636 on Critical Infrastructure Cybersecurity works to increase information sharing from the government to the private sector, the Department of Homeland Security (DHS) is focused on expanding information sharing relationships both within the government and among the private sector through adherence to three goals:

- Build trust and credibility among critical infrastructure owners/operators;
- Build sharing relationships where no sharing is currently occurring; and
- Incorporate individual owners/operators in the sharing environment and align their cybersecurity and risk management requirements with existing and emerging data flows being developed or optimized.

For example, through the Cyber Information Sharing and Collaboration Program (CISCP), DHS has entered into Cooperative Research and Development Agreements with critical infrastructure owners and operators that enable regular and trusted sharing of actionable cybersecurity threat indicators that are immediately used for computer network defense activities. Additionally, DHS has long served as the Sector Specific Agency for both the Information Technology and Communications sectors (as well as eight other sectors). This trusted partnership with private sector and Federal partners has enabled further collaborative initiatives such as the Information Technology Sector Risk Assessment, the Cybersecurity Evaluation Program, which conducts voluntary cybersecurity assessments across all critical infrastructure sectors, and the Critical Infrastructure-Cyber Security program that leads efforts with public and private sector partners to promote an assured and resilient U.S. cyber infrastructure.

The Department also has established close working relationships with industry through partnerships like the Protected Critical Infrastructure Information (PCII) Program, which enhances voluntary information sharing between infrastructure owners and operators and the government. Furthermore, DHS conducts daily operational, information sharing, incident response, and technical assistance through the National Cybersecurity and Communications Integration Center (NCCIC) and its components: the United States Computer Emergency Readiness Team, the Industrial Control Systems Cyber Emergency Response Team, and the National Coordinating Center for Communications. Presently, the DHS Science and Technology Di-

rectorate (S&T) has ongoing or proposed cooperative activities in the area of cyber security research and development (R&D) to promote the benefits of networked technology globally, and a secure, reliable, and interoperable cyberspace.

Information Sharing and Analysis Centers (ISACs) are key partners in these efforts because they, along with similar not-for-profit and commercial entities, are able to serve as trusted providers of data from DHS to their members/customers and to other ISACs and like organizations. In turn, they serve as aggregators as well as anonymizers of their relevant member/customer cybersecurity threat data and provide threat data back to one another without attribution to the source of the data. DHS is supportive of and regularly coordinates with these partners as one way to promote private to private information sharing.

The key incentive for all participants in this type of data flow is the potential for generating increased, actionable situational awareness where the individual participants benefit from the experiences of the whole. The ability to achieve visibility of threats that are exploiting other sectors or organizations before that particular threat or a variant of that threat manifests in your networks or systems is a benefit available to all participants. We currently have more than 35 companies, ISACs, and like organizations who are participating in data sharing in this fashion, with more than 50 companies in negotiations to join that program effort, and we do not feel we need to offer specific incentives to join in these types of partnerships with the Government.

In response to the EO the DHS and the Departments of Commerce and Treasury provided recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, identifying potential incentives that could be considered as we move forward in this space. Since the agencies submitted their reports, the White House has completed the interagency review process and determined a path forward. Existing programs and authorities are currently under review to determine how we and other Departments can enable more private-to-private and private to government information sharing. As mentioned previously, we have successful models with some ISACs and the CISCP and are looking to expand on that basis and since Congress has previously granted authorities that may be able to be utilized to provide liability protection and address other legal concerns. We do know the administration is looking at a package of incentives outside information sharing for companies that adopt the framework; however, private sector response to development efforts for the framework has been largely positive, and we anticipate that many companies will adopt it without an accompanying incentives package.

Question 4. As Secretary of Homeland Security, you were an advocate for the administration's cybersecurity legislation. And last August, when the U.S. Senate considered the Cybersecurity Act of 2012, you urged its passage. I agree with statements you made last year on the shared responsibility and urgency of improving cyber security. Do you still agree that cyber security is a shared responsibility that includes both the public and private sector? What is the role of the Information Technology (IT) sector in this shared responsibility and why did you support a carve-out for the IT sector?

Answer. Yes. Cybersecurity is a shared responsibility that includes efforts from both the public and private sectors. Industry and the government have a long history of working together to protect the physical security of many critical assets that reside in private hands, from airports and seaports to national broadcast systems and nuclear power plants. There is no reason we cannot work together in the same way through a shared responsibility to protect critical infrastructure cyber systems upon which so much of our economic well-being, national security, and daily lives depend.

The statement in EO 13636 regarding IT products and services reflects our consistent philosophy that cybersecurity standards must be technology neutral, and that the government should not dictate what IT components critical infrastructure owners and operators use in their systems. Furthermore, classifying any product or service as critical infrastructure simply because it is used by critical infrastructure would dilute our efforts to identify the entities whose incapacitation by cyber incident could cause catastrophic economic or national security consequences. We are closely engaged with the IT sector to ensure that critical infrastructure owners and operators across all sectors have the market choices to secure their systems.

Question 5. Without additional statutory authority and congressional direction, the information sharing program is little more than directing executive departments and agencies to expedite the sharing of existing information. More importantly, the Executive order focuses only on the sharing of information from the government to

the private sector. How do you intend to increase the sharing of information from industry to the government, and within and among industries?

Answer. Through the Critical Infrastructure Information Sharing, Analysis, and Collaboration Program, DHS has entered into Cooperative Research and Development Agreements with critical infrastructure owners and operators that enable regular and trusted sharing of actionable cybersecurity threat indicators that are immediately used for computer network defense activities. Additionally, DHS has long served as the Sector Specific Agency for both the Information Technology and Communications sectors. This trusted partnership with private sector and Federal partners has enabled further collaborative initiatives such as the Information Technology Sector Risk Assessment, the Cybersecurity Evaluation Program, which conducts voluntary cybersecurity assessments across all critical infrastructure sectors, and the Critical Infrastructure-Cyber Security program that leads efforts with public and private sector partners to promote an assured and resilient U.S. cyber infrastructure.

It is important to note that the Executive order directs Federal agencies to work within current authorities and increase voluntary cooperation with the private sector to provide better protection for computer systems critical to our national and economic security. It does not grant new regulatory authority or establish additional incentives for participation in a voluntary program. We continue to believe that a suite of legislation is necessary to implement the full range of steps needed to build a strong public-private partnership, and we will continue to work with Congress to achieve this.

The Department also has established close working relationships with industry through partnerships like the Protected Critical Infrastructure Information (PCII) Program, which enhances voluntary information sharing between infrastructure owners and operators and the government. Furthermore, DHS conducts daily operational, information sharing, incident response, and technical assistance through the National Cybersecurity and Communications Integration Center (NCCIC) and its components: the United States Computer Emergency Readiness Team, the Industrial Control Systems Cyber Emergency Response Team, and the National Coordinating Center for Communications. Every day partners from private sector critical infrastructures, Information Sharing and Analysis Centers, Federal cybersecurity centers, and international governments collaborate on cybersecurity response and information sharing through the NCCIC. These activities take place voluntarily, and in recognition of the fact that DHS' unique positioning as the hub for cybersecurity and critical infrastructure security and resilience makes it the most effective and trusted point of coordination and collaboration for all of those stakeholders.

Additionally, the DHS Science and Technology Directorate (S&T) has formalized 13 international bilateral agreements that allow for cooperative activities in the area of cyber security research and development (R&D) to promote the benefits of networked technology globally, and a secure, reliable, and interoperable cyberspace.

Question 6. The definition of critical infrastructure in the President's Executive Order (EO) is very broad: "systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." It is hard to imagine any industrial sectors that would be excluded from such a definition. How do you balance security with practicality in implementing this definition?

Answer. The term "critical infrastructure" is statutorily defined and this language has since been the basis for critical infrastructure protection activities, including Executive Order (EO) 13636. The Department of Homeland Security (DHS) has conducted broad engagement with critical infrastructure owners and operators over the past ten years that has enhanced the security and resilience of our Nation's infrastructure.

Under Section 9 of EO 13636, the Department will identify a list of critical infrastructure whose incapacitation from a cyber incident would have *catastrophic* public health and safety, economic or national security consequences. This is a higher threshold than *debilitating* consequences and will focus on a small subset of U.S. infrastructure, not entire sectors.

This is a criticality-based approach, and will result in limited Federal resources being focused on critical infrastructure, the failure of which would pose the greatest hazards.

Question 7. Section 10 of the Executive order directs all sector-specific agencies to make the Framework mandatory for their respective sectors of industry. Do you believe that the veiled threat of mandatory standards with few, if any, strong incentives is the right formula for a successful public-private partnership?

Answer. With today's physical and cyber infrastructure more inextricably linked, critical infrastructure and emergency response functions are inseparable from the information technology systems that support them. The government's role in this effort is to share information and encourage enhanced security and resilience, while identifying and addressing gaps not filled by the market-place. While some companies have strong cybersecurity policies in place, others still need to implement improved cybersecurity practices. The framework will be developed collaboratively with industry and will incorporate existing international standards, practices, and procedures wherever possible.

Section 10 of EO 13636 refers to "Agencies with responsibility for regulating the security of critical infrastructure," which in general are not sector-specific agencies (SSAs). Not generally having regulatory authority, the SSAs are better able than regulators to engage in partnership with industrial sectors. Moreover, EO 13636 only directs existing regulators under current authorities to examine ways to increase their sector's cybersecurity; any mandatory participation here would occur only where regulators already have the authority to impose security requirements on their respected regulated entities. The aim is not to compel across-the-board participation, even if such authorities did exist. Even then, EO 13636 does not dictate a "one-size fits all" approach, but rather promotes collaboration to encourage innovation and recognize differing needs and challenges within and among critical infrastructure sectors. Specifically, section 8(d) of the EO requires the Secretaries of Homeland Security, Treasury and Commerce to each make recommendations on a set of incentives designed to promote participation in the voluntary cybersecurity framework. The Department of Homeland Security (DHS) is working collaboratively with industry as well as staff from Treasury and Commerce to further develop these recommendations, and the incentives found in this report will also inform the larger nation-wide conversation. While DHS can make recommendations, only Congress has the authority to provide strong incentives and agree with or implement any recommendations put forward from the three Incentives Reports.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RON JOHNSON TO HON. JANET NAPOLITANO

Question 1. The Government Accountability Office (GAO) issued a report in February 2013 entitled, "National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented." In this report GAO found that only eight of 22 of agencies were in compliance with risk management requirements under the Federal Information Security Management (FISMA) standards in 2011, down from 13 out of 24 in 2010. Yet the Federal Government reported 782 percent more cyber incidents to the U.S. Computer Emergency Readiness Team in 2012 than it did in 2006. What is DHS doing to achieve greater compliance with FISMA standards from Federal agencies? How does the increase in cyber incidents against the Federal Government, combined with the decrease in compliance of Federal agencies with FISMA, impact the cybersecurity posture of the U.S. Government?

Answer. The Department of Homeland Security's (DHS) role in the implementation of the Federal Information Security Management Act of 2002 (FISMA) is delineated by Office of Management and Budget (OMB) guidance. Under current authorities, DHS can only monitor, recommend security posture improvements, and report on Federal agencies' compliance with FISMA. As the Government Accountability Office (GAO) report notes, the current law should be updated to give DHS the statutory authority it needs to fulfill the responsibilities it has been given. The Administration's May 2011 legislative proposal to Congress included provisions that would address this issue. The Administration continues to support legislation that would update Federal agency network security laws, and codify DHS's cybersecurity responsibilities.

While FISMA did not envision the scope of today's emerging threats and cybersecurity challenges, DHS is pursuing a number of initiatives such as Continuous Diagnostics and Mitigation (CDM), Trusted Internet Connections, and the Einstein programs to strengthen cyber security defenses, visibility and situational awareness.

In collaboration with the National Security Staff (NSS) and OMB, DHS uses its expanded CyberStat program to perform intense, focused reviews with the 24 Chief Financial Officers Act agencies to identify and mitigate challenges to agencies' FISMA implementation. This includes a plan of action and milestones, submitted by the agencies and accepted by NSS, OMB, and DHS, outlining the approach to correct identified deficiencies.

Congress provided funding in the DHS Appropriations Act, 2013 (P.L. 113–6) to implement Continuous Diagnostics and Mitigation (CDM) across civilian Executive Branch agencies in order to increase our ability to identify and track threats, find vulnerabilities, mitigate issues and report on progress. Earlier appropriations initiated other DHS security programs.

DHS continues to encourage Congress to pursue legislation that would result in:

- Improved security posture leading to improved regulatory compliance;
- Standardized security configurations across critical infrastructure;
- Improved communication and collaboration methods across diverse stakeholder groups;
- Improved situational awareness, which creates synergy among elements of the cybersecurity workforce; improves communication and facilitates information sharing; and
- Increased efficiency and security posture through collaboration and streamlining.

Question 2. GAO found that DHS is not successfully detecting, responding to, or mitigating cyber incidents. Specifically, GAO raised concerns with how DHS shares information among Federal agencies and the private sector. The DHS OIG recommended that DHS establish a "consolidated, multiple-classification-level portal to share incident response related information," but DHS will not have this portal ready until 2018. How will not having this capability until 2018 impact DHS' role in sharing cyber threat information, as directed in the Executive order?

Answer. GAO–13–187 highlights important challenges facing Federal agencies, including DHS, in executing the cyber mission. The report also highlights the significant and important progress DHS and other agencies have made in advancing this mission.

As a result of the progress DHS has made in information sharing and analysis, GAO closed each of the 10 recommendations under its Cyber Analysis and Warning report. Furthermore, DHS provided GAO with all documentation requested to close the remaining recommendations under GAO's report titled Key Private and Public Cyber Expectations Need to be Consistently Addressed. The National Cybersecurity Protection System's information-sharing and collaboration environment will address the recommendation to establish a consolidated multi-classification information-sharing capability. Funding for this activity is included in the President's Fiscal Year 2013 budget request. While continuing the development of a comprehensive information sharing capability is important, DHS maintains existing capabilities that allow for information exchange with private sector partners at the classified and unclassified levels facilitating DHS' role in sharing cyber threat information, as directed in the Executive order.

The delay in implementation may impact the frequency and timeliness with which DHS is able to exchange classified cyber information with partners. Processes leveraged as a workaround until the portal reaches FOC may be cumbersome to analysts and reduce the amount of time available to conduct strategic analysis across classified and unclassified domains. As a result, partners may find other sources for similar information, which could result in a decrease in their willingness to engage in the Department's various information sharing initiatives.

Existing NCPS Information Sharing capabilities will be improved and new capabilities will be brought online as the Information Sharing environment matures. The NCPS Information Sharing CONOPs identifies multiple information sharing capabilities. A capability roadmap has been developed that identifies dependencies and specifies how these capabilities will be acquired and implemented. Initial Operating Capability for this set of capabilities is targeted for FY 2015. Full Operating Capability, which includes integration of capabilities and automation of processes across multiple security fabrics, will occur in FY 2018.

Question 3. GAO found that the Federal Government's strategy for addressing international cyber security challenges is not sufficient or outcome oriented. GAO also recommended that the White House Cybersecurity Coordinator develop an overarching Federal cybersecurity strategy. GAO indicates that such a strategy would hold Federal agencies accountable for making improvements in their own house, and would address international cybersecurity challenges. Do you agree with the White House that an overarching Federal cybersecurity strategy is unnecessary? Why or why not?

Answer. The Department of Homeland Security (DHS) executes a whole-of-government and whole-of-nation approach to cybersecurity. In support of this, DHS has aligned its cybersecurity goals, initiatives, and objectives to be consistent with the Administration's priorities for protecting our Nation's critical information infrastruc-

ture and building a safer and more secure cyber ecosystem. For instance, DHS worked closely with Federal departments and agencies in developing the *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise (Blueprint).* The *Blueprint* leverages the Comprehensive National Cybersecurity Initiative, the President's *2010 National Security Strategy,* the Department of Defense's *Strategy for Operating in Cyberspace,* and the President's *International Strategy for Cyberspace.* Together, these documents take a whole-of-government approach and reinforce the need for holistic thinking about the many opportunities and challenges the Nation faces in cyberspace.

Question 4. In Mr. Gallagher's testimony he pointed out the difference between "standards" and "regulations." Do you agree with Mr. Gallagher that there is a difference between standards and regulations?

Answer. Yes, the Department of Homeland Security agrees that there is a difference between standards and regulations. Regulations are mandatory and binding on regulated parties as required by a particular authority. Executive Order (EO) 13636 does not give any Federal entity new authority to impose regulations or mandates on critical infrastructure owners and operators. One of the many goals of this EO and Presidential Policy Directive 21 (PPD 21) is to better streamline the government's interactions with critical infrastructure owners and operators and state, local, tribal, and territorial partners.

The EO directs the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. The Framework will be created using standards, guidelines, and best practices that promote the protection of information and information systems supporting critical infrastructure operations. Standards are voluntary recommendations established by consensus and are recognized by a standardization body. NIST will ask stakeholders to identify existing cybersecurity standards, guidelines, frameworks, and best practices that are applicable to increase the security of critical infrastructure sectors and other interested entities. Regulators of critical infrastructure operations are encouraged to share their insight and help identify existing standards already developed by industry through consensus. Those activities would support the development of the framework and prove useful in identifying any gaps in current practices given the current and projected cyber risks. Entities that are unregulated—or where regulators determine that they do not have the ability under existing law to regulate for cybersecurity—will be encouraged to voluntarily adopt the framework.

Question 5. Mr. Gallagher stated in his that any approach to cybersecurity should not "dictate solutions to industry, but rather facilitate(s) industry coming together to develop solutions." Do you agree that any approach to a Cybersecurity Framework should not "dictate" solutions to industry but rather "facilitate industry coming together to develop solutions?" What potential disadvantage would there be to government dictating a solution to industry rather than facilitating it?

Answer. Yes, the Department agrees that any approach to the Cybersecurity Framework should "facilitate industry coming together to develop solutions."

The Framework will not dictate "one-size fits all" technological solutions. Instead, it will promote a collaborative approach to encourage innovation and recognize differing needs and challenges within and among critical infrastructure sectors. The Government believes that companies driving cybersecurity innovations can help shape best practices across critical infrastructure, in part because of the changing nature and dynamic of risk across cyber and critical infrastructure. Companies looking to strengthen their security would have the flexibility to decide how best to do so using innovative products and services available in the marketplace and choosing which components of the Framework would apply to their business. Companies that are cyber leaders will be looked to as models for implementing best practices and driving the creation and implementation of a Cybersecurity Framework itself.

Question 6. GAO found that Federal cyber strategies lack clear goals, performance measures, defined costs and resources, established roles and responsibilities, and do not coordinate with other national strategies. Yet the EO directs DHS to use a "risk-based" approach to identify "critical infrastructure" within 150 days. The EO also directs DHS to develop performance measures associated with the Cybersecurity Framework NIST is charged with developing. If Federal cyber strategies lack goals and performance measures, what experience does it have to draw on to develop performance measures for the private sector, as directed in the EO?

Answer. The Department's *Blueprint for a Secure Cyber Future* has specific goals and performance measures associated with it. That said, Section 7(d) of Executive Order (EO) 13636 directs the Department of Homeland Security (DHS) to provide "performance goals"—not performance measures—in connection with the Cybersecu-

rity Framework that is being prepared by the National Institute of Standards and Technology (NIST). Critical infrastructure owners and operators that adopt the goals would then develop their own measures and targets since each sector and subsector has unique characteristics and each owner/operator is in the best position to tailor the performance goals to its business model. Separately, NIST's Cybersecurity Framework will include guidance for measuring the performance of an entity as it implements the framework. NIST has considerable experience developing similar guidance through its special publications, and the draft Framework is being developed through extensive consultation with industry. Further, they are able to influence the effort through their direct engagement and input.

Question 7. Why do you believe Federal cyber strategies have failed to include clear goals, performance measures, defined costs and resources, established roles and responsibilities, and to coordinate with other national strategies?

Answer. Legacy Federal cyber strategies were developed by different agencies at different points in time. However, beginning with the Comprehensive National Cybersecurity Initiative in 2008, which was followed by the Administration's Cyberspace Policy Review in 2009, Federal cyber strategies have increasingly been developed through interagency processes and with the attributes identified above. For example, DHS helped lead development of "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program." In another example, DHS's *Blueprint for a Secure Cyber Future* contains goals against which the Department's cybersecurity programs align performance measures, milestones, resources, roles and responsibilities. Future year budget requests and performance measures for emerging programs are developed in alignment with the *Blueprint.* In addition to the *Blueprint,* the Administration's international cyber strategy, and the Department of Defense's cybersecurity strategy provide the architecture of ongoing initiatives upon which EO 13636 and Presidential Policy Directive (PPD) 21 are being implemented. With the issuance of EO 13636 and PPD–21, the Administration is providing an opportunity for the Department, other Federal, state and local agencies, and the private sector to discuss and prioritize cybersecurity measures to improve critical infrastructure cybersecurity and ensure overall critical infrastructure security and resilience. These actions direct the Department to create performance goals, consider resourcing, and work with and update national strategies, which will also outline roles and responsibilities for these efforts.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. KELLY AYOTTE TO HON. PATRICK D. GALLAGHER

Question. I've recently read that some CIOs would have higher comfort levels managing cyber security with cloud computing because vendors such as Google and salesforce.com have vastly more resources to protect against cyber threats than smaller companies do. Do you believe and Executive Order or a cyber bill would limit a company's ability to farm out their cyber security needs? Can you address in more detail your thoughts on cloud computing as it relates to cybersecurity?

Answer. Cloud computing is a powerful option that, when implemented correctly, allows businesses to use information technology services to meet their business needs while protecting their assets. Cloud computing can provide cybersecurity capabilities that organizations might find more cost-effective and often allow more resources to provide cybersecurity than the organizations might be able to provide themselves. This is generally a measurement of each side's cybersecurity capability, the services offered by the Cloud provider, the cost to provide those services, and the level of needed assurance and visibility of those services by the customer.

The Executive Order requires that "the Cybersecurity Framework will provide guidance that is technology neutral". As such, the Framework will not limit or put constraints on a company's ability to use a Cloud service provider to meet their needs. The Framework will not require or limit a specific architecture or implementation model.

Under its responsibilities in the Federal Information Security Management Act (FISMA), NIST has published several public cybersecurity guides and recommendations on the cybersecurity capabilities of cloud technologies, as well as guidance on cybersecurity considerations when using cloud service providers. NIST also works jointly with other agencies in the Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

More detailed information on the NIST work in cloud computing and cybersecurity can be found at the below links:

www.fedramp.gov
www.nist.gov/itl/cloud/
http://www.nist.gov/itl/cloud/publications.cfm

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DAN COATS TO HON. PATRICK D. GALLAGHER

Question. NIST is tasked with developing the framework outlined in the EO, which I think is appropriate given NIST's technical expertise. Does NIST have the capacity to develop this framework utilizing its existing resources?

Answer. Yes. Given that NIST's philosophy is that industry should lead the development of the Framework, NIST's role with the Framework will be primarily to convene and provide technical expertise, instead of developing new standards and solutions. This "bottom-up" approach allows NIST to leverage existing resources, and is similar to its work with industry to address national priorities in a range of topics, ranging from smart grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips.

Going forward, our process will continue to be an open one—using an approach to enhance cybersecurity across the sectors through industry consensus. NIST's process will be focused on developing the Framework in such a manner that the standards and practices can apply to the range of sectors, with a full range of operational and business needs. That will allow for increased engagement and flexibility, both for the standards and practices that comprise the framework and for the evolving nature of the threat.

In addition to existing resources, in the Administration's FY14 Budget request NIST has an increase of $2M for cybersecurity standards that will support the framework being developed under the Executive Order on Improving Critical Infrastructure Cybersecurity.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RON JOHNSON TO HON. PATRICK D. GALLAGHER

Question 1. I was pleased to read in your testimony that the Cybersecurity Framework NIST is charged with developing will be "NIST-coordinated and industry-led." How can we ensure that the best practices and standards industry already has and is developing are utilized in this Framework?

Answer. Through a request for information (RFI), NIST asked stakeholders a series of questions about existing standards, practices, and frameworks. NIST received 244 responses to the RFI including responses from individuals, industry groups and associations (to show consensus) and organizations (to be able to provide additional detail on particular responses). NIST will also be hosting a series of workshops to gather more information and develop the Framework, to ensure that those existing standards and best practices are incorporated, and where potential gaps might exist. The first will be held at Carnegie Mellon Campus in Pittsburgh on May 29–31, followed by additional workshops around the country on the weeks of July 15 and September 9. The draft Framework will also be posted for another round of comment by October 10. In between each workshop NIST will publically present findings to ensure additional collaboration.

Question 2. What can be done to ensure that the voluntary program DHS is charged with developing for participation in this Framework does not turn into a mandatory regulatory structure?

Answer. The Executive Order (E.O. 13636—Improving Critical Infrastructure Cybersecurity) states that the program established by the Department of Homeland Security in coordination with Sector-Specific Agencies shall be voluntary. NIST plans on discussing issues relating to long-term public-private governance to ensure that the framework stays flexible and effective in the dynamic environment of threats and new technologies. The EO encourages voluntary participation and adoption and provides for harmonization among existing regulatory requirements.

Question 3. Your testimony states that any approach to cybersecurity should not "dictate solutions to industry, but rather facilitate(s) industry coming together to develop solutions." Do you believe that mandatory regulations in a future Cybersecurity Framework equate to the government dictating a solution to industry?

Answer. Some sectors—but not all—of our most critical infrastructure already fall under cybersecurity regulation. The RFI issued by NIST asked a variety of questions about those regulated sectors, to ensure that the Framework would be applicable for parts of industry. In addition, the executive order itself calls for a review of existing cybersecurity regulation. For those sectors, regulatory agencies will use the Cybersecurity Framework to assess whether existing requirements are sufficient to protect against cyber attack. If existing regulations are insufficient or ineffective, then agencies must propose new, cost-effective actions based upon the Cybersecurity Framework. Regulatory agencies will use their existing process to consult with their regulated companies to develop and propose any new regulations, allowing for a collaborative process.

Question 4. You state in your testimony that standards are "agreed-upon best practices against which we can benchmark performance. Thus, these are NOT regulations." Can you tell us more about the difference between standards and regulations? Why do you make such a point of clarifying that standards are NOT regulations?

Answer. Standards are developed in a consensus process with stakeholders and are voluntary. Technical regulations are set by an authority and are mandatory. My testimony makes that distinction in order to specify that the process under the Executive order will build on the existing solutions that are already used throughout industry, instead of generating regulations. The Executive Order specifies that the Framework must meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), and OMB Circular A–119, as revised—all laws and policy that dictate how the Federal Government uses standards and participates in standards development.

Question 5. What downside is there to turning industry standards into mandatory regulations in a Cybersecurity Framework?

Answer. Having industry standards as a part of the Cybersecurity Framework would not turn them into mandatory regulations. The development of the Framework will be done in such a way to encourage adoption of existing standards—focusing on practices that will enhance the security of organizations that easily fit in their current business practices. We expect the Framework to have tools that will satisfy different regulatory and legal requirements with an "implement once, comply many" mentality. This would lower regulatory compliance costs while allowing organization to focus on risk management.

Question 6. Given your experience, how can the International Organization for Standardization be leveraged to develop voluntary standards for what will be deemed cyber critical infrastructure?

Answer. The International Organization for Standardization is one of many industry led, consensus based, transparent Standards Development Organizations (SDOs) that operation in a multinational environment. This type of SDO is essential for large scale, global adoption where both our critical infrastructures and those that supply them with critical IT and equipment operate in a global market.

NIST will work with the stakeholders in a public-private partnership on the development of the framework and will identify both when and where the framework or components of the framework are ready for further development as international standards.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. AMY KLOBUCHAR TO DAVID E. KEPLER

Question 1. I think it's important to recognize the proactive steps industry has undertaken to invest in cyber security and independently develop programs and best practices to protect their networks, operations and customers. Do you believe privately-held critical infrastructure companies have a responsibility to secure themselves and their customers from cyber threats to the maximum extent possible?

Answer. Yes, cybersecurity risk is important and should be managed by all companies. Companies are limited by the amount of cyber intelligence that government shares, quality and security of IT products, and services provided by the telecommunication sector. These should be an area of emphasis for any new cyber security legislation.

Question 2. I appreciate the efforts Dow and the American Chemistry Council have made. Are other major critical infrastructure sectors and companies making similar investments in implementing cyber security procedures and promoting best practices among their employees?

Answer. We do not have direct exposure to the initiatives of other sectors.

Question 3. Dow Chemical is, of course, a major company with substantial resources to devote to this problem. Do all critical infrastructure sectors and companies have the same level of resources to devote to cyber security?

Answer. We are unable to comment on this.

Question 4. Do all critical infrastructure sectors and companies share the same deep knowledge and appreciation of the seriousness of cyber security threats as you and your company?

Answer. We have participated in some industry forums where other sectors have shared their approach to address cyber security. It seems to be an important risk for American companies.

Question 5. If not all critical infrastructure sectors and companies share the same will and capability to address this threat, does the Federal Government have a responsibility to do something to direct or assist measures to protect that critical infrastructure?

Answer. We do support legislation that promotes information sharing and provides liability protection. In addition to that, legislation should address the accountability of IT and telecommunication suppliers to produce secure products and be unified in providing services that companies can rely on for threat response. Government, IT industry and telecommunications are the backbone of the internet.

Question 6. Are there inter-sector efforts among private critical infrastructure providers to help one another develop cyber security procedures and best practices? It would seem that all sectors and companies ought to be able to agree on some investments in this area that are necessary and wise.

Answer. ACC has been promoting information sharing among chemical companies and has defined cyber security expectations for companies that are part of ACC and the Responsible Care program. We do not actively collaborate with other sectors.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN COATS TO DAVID E. KEPLER

Question 1. The EO, as I read it, focuses solely on government-to-private-sector information sharing. My sense is that better private-to-government and private-to-private information sharing protocols need to be implemented, and I question how we can get there without better liability protections. What would you need for better private-to-government and private-to-private information sharing?

Answer. Experience would indicate that most of the critical infrastructure sectors have good private-to-private information sharing protocols that have been developed in their industry groups. However, cross industry, regional and national private-to-private information sharing could be improved. The following capabilities would help improve information sharing:

- A well-established protocol on how information will be recorded and stored.
- Clarity on which individuals can receive information.
- Relief from liability for information sharing, provided a proper management system is in place, and liability protection for the private sector as a result of a cyber-attack, as afforded under the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002.
- Protocol on managing anti-trust and FOIA requests.

Question 2. Expertise in cybersecurity is a formula (expertise = technical capability + cyber threat information). Where do you turn for expertise now and how might that change under the President's Executive Order? Do you feel private sector cybersecurity is lacking technical capability or cyber threat information?

Answer. There has been significant investment in technical skills, expertise and technologies in the chemical industry and at Dow, specifically. We find this to be true in most large companies and critical infrastructure industries. There has also been strong engagement in standard setting. We benchmark and share information with our industry, across industries, with government agencies and with IT and security suppliers. It is not clear to us that this is changing with the Executive order.

The one area we think the Executive order falls short is how it will address the information technology community. Effective cyber information sharing policy should be comprehensive in its coverage of all relevant industry parties including the IT sector.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARCO RUBIO TO DAVID E. KEPLER

Question 1. The National Infrastructure Advisory Council (NIAC) provides the President and Secretary Napolitano with advice on the security of the critical infrastructure sectors and their information systems. Based on your experience at the council, are you aware of current programs or efforts that could be leveraged to combat cyber threats, rather than setting up a completely new framework and set of standards?

Answer. Cybersecurity policies were set back in 2003 for the nation, with the National Strategy to Secure Cyberspace, and many programs such as NIPP and CFATS in the chemical sector to address cybersecurity. In addition, there are standards already in place that industry is engaged in and implementing, such as ISO 27002 and ISA/IEC 62443 for industrial automation. We would encourage the Administration to engage with industry sectors to build on the systems in place rather than starting from scratch.

Question 2. Dow is one of the largest manufacturers of chemicals in the world and a multinational corporation that has its own cybersecurity standards and protections in place. Dow has also invested significantly in its own infrastructure to combat cyber threats. Now the Federal Government is setting up a framework with standards and best practices. This is after there was legislation in the last Congress that would have taken the role of government a step further. As a company with cybersecurity protections in place, with a vested interest in protecting your networks and assets, what do you feel is the proper role of government with regards to cybersecurity?

Answer. The role of government is to set effective national security policy. The focus of an Executive Order or legislation should be:

- Manage government networks according to its own standards.
- Ensure that the information technology suppliers are working with the communication suppliers and government to harden basic Internet security.
- Create an environment to safely share information between the government and private sector.
- Aggressive pursuit and prosecution of cyber criminals (including international crime).

Question 3. Your testimony states that Dow has concerns with the Executive order's current approach of a voluntary program for critical infrastructure industries to adopt cybersecurity standards. Is there a concern that government defined standards or selected standards could miss the specific challenges faced by the chemical industry? Dow operates in a dynamic environment and cyber threats are always changing and take on different forms. Why it is important for the voluntary standards to be flexible? Could a static government requirement inhibit your ability to respond to threats?

Answer. The industry already works under standards and protocols, such as ISO 27002 and ISA/IEC 62443 for industrial automation, as well as the Responsible Care Security Code, that are not only voluntary but are required to maintain membership in the American Chemistry Council.

There is a concern that there will be documentation and publication of any industry or company within critical infrastructure if they choose not to volunteer to a standard. There will be legitimate debate on specific risks and why a variance should be applied or how it should be applied. For example, cyber standards without imbedding and understanding the physical standards and other mitigations do not show the complete mitigation effort.

Effectively, setting pseudo regulations may stifle superior cybersecurity systems by impeding quick response or system specific security.

Question 4. There has been criticism in Congress directed at the private sector for not doing enough to combat cyber threats. Yet the GAO just found a disturbing trend that Federal agencies are failing to comply with Federal Information Security Management standards, and that DHS has not adequately met its responsibilities. Is Dow alarmed that some of the very agencies that may require more of the company with respect to cybersecurity have been found to be lacking in their own cyber standards and practices?

Answer. Yes, a key point is that government should play a more constructive role in setting an example of securing their own networks, sharing information, as well as setting standards for the IT suppliers to help them rather than revisiting critical infrastructure compliance.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RON JOHNSON TO DAVID E. KEPLER

Question 1. How is Dow Chemical, and the chemical industry in general, currently hampered from sharing information among peers and with the government?

Answer. We need legislation that covers liability protection for sharing threat or attack information with the government and antitrust relief to share with industry peers.

Question 2. How important is it to your industry for Congress to pass information sharing legislation?

Answer. It is very important for the industry that government shares more information on cyber security threats and best practices. We fully rely on the government's capabilities. The private sector does not have the resources or expertise to support cyber intelligence activities.

Question 3. Would you prefer for Congress to attempt to pass a comprehensive piece of cybersecurity legislation or to attempt to address the low-hanging fruit in a piecemeal fashion?

Answer. We do support a "piecemeal, low-hang fruit approach" like addressing information sharing. In addition to that, legislation should address the accountability of IT and telecommunication suppliers to produce secure products and be unified in providing services that companies can rely on for threat response. Government, IT industry and telecommunications are the backbone of the internet.

Question 4. Mr. Gallagher's testimony stated that any approach to cybersecurity should not "dictate solutions to industry, but rather facilitate(s) industry coming together to develop solutions." Do you believe that mandatory regulations would equate to the government dictating a solution to industry?

Answer. Yes, the industry sector does not need prescriptive solutions. All solutions should be risk-based considering the characteristics and the dynamics of different industries. We agree that any approach to cyber security should create an environment where government, IT industry, the telecommunications sector and other industries can collaborate to elevate the overall security of the country.

Question 5. You stated in your testimony that Dow adheres to a set of policies and standards from organizations including NIST and established industry standards set forth by the International Organization for Standardization (ISO). Given your experience, how can the ISO be leveraged to develop voluntary standards for what will be deemed cyber critical infrastructure?

Answer. We believe that companies, especially critical infrastructure companies, should implement cyber security programs that comply with accepted industry practices like ISO 27001. Some of the companies are multinational, and ISO 27001 standards allow global implementations.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RON JOHNSON TO GREGORY C. WILSHUSEN

Question 1. The Government Accountability Office (GAO) issued a report in February 2013 entitled, "National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented." In this report GAO found that only eight of 22 of agencies were in compliance with risk management requirements under the Federal Information Security Management (FISMA) standards in 2011, down from 13 out of 24 in 2010. Yet the Federal Government reported 782 percent more cyber incidents to the U.S. Computer Emergency Readiness Team in 2012 than it did in 2006. How does the increase in cyber incidents against the Federal Government, combined with the decrease in compliance of Federal agencies with FISMA, impact the cybersecurity posture of the U.S. Government?

Answer. Threats to systems supporting critical infrastructure and Federal operations are evolving and growing, and the increasing risks are demonstrated by the dramatic increase in reports of security incidents. However, several factors make it difficult to directly correlate the number of reported incidents with the overall cybersecurity posture of the U.S. Government. For example, according to the United States computer emergency readiness team (US–CERT), the growth in the total number of reported incidents is attributable, at least in part, to agencies improving their detection and reporting of security incidents on their networks. Further, having better detected incidents, it is possible that agencies are also better implementing appropriate responsive and preventative countermeasures. We have ongoing work to assess agencies' incident response and handling procedures. As we reported, agencies are still challenged in implementing several aspects of their information security programs, including risk management. To help address short-

comings in risk management, the administration has set a cross-agency priority goal to improve continuous monitoring. Continuous monitoring is the process of maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Federal agencies are to achieve 95 percent implementation of a continuous monitoring program by 2014. According to the Office of Management and Budget (OMB), in Fiscal Year 2011, implementation of automated continuous monitoring capabilities rose from 56 percent of total assets in Fiscal Year 2010 to 78 percent of total assets in Fiscal Year 2011, although, as we reported, agency inspectors general cited weaknesses in continuous monitoring at a number of agencies. While the mixed results of agency FISMA implementation statistics do not clearly indicate whether the government's cybersecurity posture is deteriorating as a result of an increase in reported incidents, the overall need for agencies to improve their cybersecurity programs is clear.

Question 2. On February 12, 2013, the White House issued an Executive Order (EO) entitled "Improving Critical Infrastructure Cybersecurity." In this EO, the White House directs the National Institute for Standards and Technology to develop a Framework to reduce cyber risks to critical infrastructure. At the March 7 hearing, Mr. Gallagher stated that any such framework will be NIST-coordinated but industry-led in order to draw on standards and best practices from industry. He went on to say that any approach should not dictate solutions to industry but rather facilitate industry identifying solutions. How important is it for the development of the Cybersecurity Framework to be "industry-led?" Why?

Answer. The Executive Order states that the Director of the National Institute of Standards and Technology (NIST) will lead the development of the Cybersecurity Framework, and the NIST Director is accountable for publishing a final version of the framework by February 12, 2014. However, Mr. Gallagher, as noted, interpreted NIST's role to be one of coordinating an industry-led effort. This interpretation is consistent with the executive order's direction that the cybersecurity framework incorporate voluntary consensus standards and industry best practices to the fullest extent possible and employ a consultative process whereby the advice of critical infrastructure owners, among others, is considered. We believe the extent to which industry participates in developing the framework will likely influence the extent to which the framework is adopted by infrastructure owners and operators and has a positive effect in enhancing the security of the Nation's critical infrastructure.

Question 3. What are potential downfalls of having a solution be dictated from the government to industry?

Answer. Collaboration and the use of a consultative process are critical to the success of the effort to develop and facilitate adoption of the Cybersecurity Framework by critical infrastructure owners and operators. A solution dictated from the government to industry could pose risks that burdensome implementation costs could be imposed on industry, the technical aspects of the solution might be less practical or effective than other options, and industry would be reluctant to implement the framework. For these reasons, the standards-setting process in the United States, as elsewhere in the world, relies on principles of consensus, transparency, balance, due process, and openness to ensure that any framework of standards is as inclusive as possible.

Question 4. What issues, both generally and specifically, in your view should Congress perform oversight of over the next year as this Framework is developed?

Answer. The executive order specifies several activities that can provide a basis for overseeing the development and implementation of the framework. Within the next year, the emphasis will be on developing the framework. Congress can focus on overseeing NIST's implementation of the consultative process to ensure that industry is heavily involved. This oversight could include reviewing the preliminary version of the framework, which is due 240 days after the order was issued. In addition, recommendations regarding a set of incentives for promoting participation in the program are to be made within 120 days of the order's issuance. Further, within 150 days, the Secretary of Homeland Security is to identify critical infrastructure at greatest risk, using a consultative approach. Congressional oversight can include reviewing these activities to ensure that the requirements specified in the order are met.

Question 5. GAO found that Federal cyber strategies lack clear goals, performance measures, defined costs and resources, established roles and responsibilities, and do not coordinate with other national strategies. This failure to coordinate strategies raises concerns over how effective the Administration can be in implementing the new responsibilities laid out in the Executive order. The EO directs DHS to use a "risk-based" approach to identify "critical infrastructure" within 150 days. The EO also directs DHS to develop performance measures associated with the Cybersecuri-

ty Framework NIST is charged with developing. If the government is having a hard time developing performance measures for itself, how will this impact the government's ability to develop performance measures for the private security? How involved should industry be in this process?

Answer. Without a proven track record for developing performance measures, the Federal Government will need to engage the private sector to help develop private sector performance measures. While the government has generally not included performance metrics in its national strategy documents, it has developed metrics for measuring the implementation of security controls by Federal agencies. For example, the Department of Homeland Security (DHS) has developed the metrics used in the Cyberscope reporting tool, which captures data on security control implementation at agencies, although it generally did not include a metric that addresses performance targets which would allow agencies to track progress over time. Our report on information security performance measures demonstrated that leading organizations used compliance, effectiveness of controls, and program impact performance metrics for monitoring their information security posture.[1]

Developing useful performance measures for the private sector's implementation of the Cybersecurity Framework, like the development of the framework itself, relies on collaboration with the private sector. Federal policy, including Presidential Policy Directive 21, Executive Order 13636, and the National Infrastructure Protection Plan (NIPP), establishes a cyber protection approach for the Nation's critical infrastructure sectors that focuses on the development of public-private partnerships. The NIPP sets forth a risk management framework and details the roles and responsibilities of DHS, sector-specific agencies, and other federal, state, regional, local, tribal, territorial, and private sector partners, including how they should use risk management principles to prioritize protection activities within and across sectors.[2] Further, the NIPP recommends that outcome-oriented metrics be established that are specific and clear as to what they are measuring, practical or feasible in that needed data are available, built on objectively measureable data, and aligned with sector priorities. Direct input from the private sector will be critically important in ensuring that these criteria are met.

[1] GAO, *Information Security: Concerted Effort Needed to Improve Federal Performance Measures,* GAO–09–617 (Washington, D.C.: Sept. 14, 2009).

[2] Presidential Policy Directive 21 directed the Secretary of Homeland Security to update the National Infrastructure Protection Plan by October 2013.